## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Legal Notice</td>
<td>1</td>
</tr>
<tr>
<td>1.1</td>
<td>Technical Support</td>
<td>3</td>
</tr>
<tr>
<td>1.2</td>
<td>Documentation</td>
<td>4</td>
</tr>
<tr>
<td>1.3</td>
<td>Documentation feedback</td>
<td>5</td>
</tr>
<tr>
<td>1.4</td>
<td>Veritas Services and Operations Readiness Tools (SORT)</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Introduction</td>
<td>7</td>
</tr>
<tr>
<td>2.1</td>
<td>Veritas Access CLI command conventions</td>
<td>7</td>
</tr>
<tr>
<td>2.2</td>
<td>About accessing the online man pages</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Admin Commands</td>
<td>9</td>
</tr>
<tr>
<td>3.1</td>
<td>admin</td>
<td>9</td>
</tr>
<tr>
<td>3.2</td>
<td>passwd</td>
<td>11</td>
</tr>
<tr>
<td>3.3</td>
<td>show</td>
<td>12</td>
</tr>
<tr>
<td>3.4</td>
<td>supportuser</td>
<td>13</td>
</tr>
<tr>
<td>3.5</td>
<td>user</td>
<td>14</td>
</tr>
<tr>
<td>4</td>
<td>Backup Commands</td>
<td>15</td>
</tr>
<tr>
<td>4.1</td>
<td>backup</td>
<td>15</td>
</tr>
<tr>
<td>4.2</td>
<td>install</td>
<td>21</td>
</tr>
<tr>
<td>4.3</td>
<td>netbackup</td>
<td>22</td>
</tr>
<tr>
<td>4.4</td>
<td>show</td>
<td>25</td>
</tr>
<tr>
<td>4.5</td>
<td>start</td>
<td>26</td>
</tr>
<tr>
<td>4.6</td>
<td>status</td>
<td>27</td>
</tr>
<tr>
<td>4.7</td>
<td>stop</td>
<td>28</td>
</tr>
<tr>
<td>4.8</td>
<td>uninstall</td>
<td>29</td>
</tr>
<tr>
<td>4.9</td>
<td>virtual-ip</td>
<td>30</td>
</tr>
<tr>
<td>4.10</td>
<td>virtual-name</td>
<td>31</td>
</tr>
<tr>
<td>5</td>
<td>CIFS Commands</td>
<td>33</td>
</tr>
<tr>
<td>5.1</td>
<td>cifs</td>
<td>33</td>
</tr>
<tr>
<td>5.2</td>
<td>homedir</td>
<td>45</td>
</tr>
<tr>
<td>5.3</td>
<td>local</td>
<td>47</td>
</tr>
<tr>
<td>5.4</td>
<td>mapuser</td>
<td>49</td>
</tr>
<tr>
<td>5.5</td>
<td>server</td>
<td>51</td>
</tr>
<tr>
<td>5.6</td>
<td>set</td>
<td>53</td>
</tr>
</tbody>
</table>
5.7 share ................................................................. 56
5.8 show ................................................................. 59

6 Cluster Commands ............................................. 61
6.1 cluster ............................................................ 61
6.2 add ................................................................. 64
6.3 del ................................................................. 65
6.4 reboot ............................................................ 66
6.5 show ................................................................. 67
6.6 shutdown ......................................................... 68

7 DB Commands ................................................... 69
7.1 database .......................................................... 69
7.2 fs ................................................................. 71
7.3 pool ............................................................... 73
7.4 share ............................................................. 75

8 FTP Commands .................................................. 77
8.1 FTP ............................................................... 77
8.2 local ............................................................. 85
8.3 logupload ....................................................... 88
8.4 server ........................................................... 89
8.5 session .......................................................... 90
8.6 set ................................................................. 92
8.7 show ............................................................... 105

9 Network Commands ........................................... 107
9.1 network .......................................................... 107
9.2 bond ............................................................ 113
9.3 device ........................................................... 116
9.4 dns ............................................................... 119
9.5 firewall .......................................................... 121
9.6 ip ................................................................. 122
9.7 krb ............................................................... 128
9.8 ldap ............................................................. 130
9.9 loadbalance ..................................................... 135
9.10 netgroup ......................................................... 136
9.11 nis .............................................................. 138
9.12 nsswitch ......................................................... 140
9.13 pcexclusion ..................................................... 142
9.14 ping ............................................................ 144
9.15 show ........................................................... 146
9.16 swap ........................................................... 148
9.17 vlan ............................................................. 149

10 NFS Commands ............................................... 151
10.1 nfs ............................................................. 151
10.2 server .......................................................... 154
10.3 share .......................................................... 156
10.4 show ........................................................... 158
10.5 stat ............................................................. 159

11 Object Access Commands .................................. 163
11.1 ObjectAccess .................................................. 163
11.2 account ........................................................ 168
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.3 bucket</td>
<td>169</td>
</tr>
<tr>
<td>11.4 group</td>
<td>170</td>
</tr>
<tr>
<td>11.5 map</td>
<td>172</td>
</tr>
<tr>
<td>11.6 server</td>
<td>173</td>
</tr>
<tr>
<td>11.7 set</td>
<td>174</td>
</tr>
<tr>
<td>11.8 show</td>
<td>176</td>
</tr>
<tr>
<td>11.9 unset</td>
<td>177</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 OpenStack Commands</td>
<td>179</td>
</tr>
<tr>
<td>12.1 openstack</td>
<td>179</td>
</tr>
<tr>
<td>12.2 cinder</td>
<td>183</td>
</tr>
<tr>
<td>12.3 manila</td>
<td>186</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 Report Commands</td>
<td>189</td>
</tr>
<tr>
<td>13.1 report</td>
<td>189</td>
</tr>
<tr>
<td>13.2 email</td>
<td>195</td>
</tr>
<tr>
<td>13.3 event</td>
<td>197</td>
</tr>
<tr>
<td>13.4 exportevents</td>
<td>200</td>
</tr>
<tr>
<td>13.5 showevents</td>
<td>201</td>
</tr>
<tr>
<td>13.6 snmp</td>
<td>202</td>
</tr>
<tr>
<td>13.7 syslog</td>
<td>204</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14 Replication Commands</td>
<td>207</td>
</tr>
<tr>
<td>14.1 replication</td>
<td>207</td>
</tr>
<tr>
<td>14.2 bwlimit</td>
<td>214</td>
</tr>
<tr>
<td>14.3 config</td>
<td>216</td>
</tr>
<tr>
<td>14.4 exclunit</td>
<td>219</td>
</tr>
<tr>
<td>14.5 job</td>
<td>221</td>
</tr>
<tr>
<td>14.6 repunit</td>
<td>225</td>
</tr>
<tr>
<td>14.7 rpo</td>
<td>227</td>
</tr>
<tr>
<td>14.8 schedule</td>
<td>228</td>
</tr>
<tr>
<td>14.9 service</td>
<td>230</td>
</tr>
<tr>
<td>14.10 sync</td>
<td>231</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 SmartIO Commands</td>
<td>237</td>
</tr>
<tr>
<td>15.1 SmartIO</td>
<td>237</td>
</tr>
<tr>
<td>15.2 cache</td>
<td>242</td>
</tr>
<tr>
<td>15.3 device</td>
<td>245</td>
</tr>
<tr>
<td>15.4 file</td>
<td>246</td>
</tr>
<tr>
<td>15.5 fs</td>
<td>248</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>16 Storage Commands</td>
<td>251</td>
</tr>
<tr>
<td>16.1 storage</td>
<td>251</td>
</tr>
<tr>
<td>16.2 cloud</td>
<td>296</td>
</tr>
<tr>
<td>16.3 compress</td>
<td>298</td>
</tr>
<tr>
<td>16.4 fencing</td>
<td>301</td>
</tr>
<tr>
<td>16.5 dedup</td>
<td>304</td>
</tr>
<tr>
<td>16.6 disk</td>
<td>308</td>
</tr>
<tr>
<td>16.7 fs</td>
<td>312</td>
</tr>
<tr>
<td>16.8 hba</td>
<td>337</td>
</tr>
<tr>
<td>16.9 iscsi</td>
<td>338</td>
</tr>
<tr>
<td>16.10 maxiops</td>
<td>349</td>
</tr>
<tr>
<td>16.11 pool</td>
<td>351</td>
</tr>
<tr>
<td>16.12 quota</td>
<td>354</td>
</tr>
<tr>
<td>16.13 rollback</td>
<td>361</td>
</tr>
<tr>
<td>Chapter</td>
<td>Section</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
<tr>
<td>16.14</td>
<td>scanbus</td>
</tr>
<tr>
<td>16.15</td>
<td>snapshot</td>
</tr>
<tr>
<td>16.16</td>
<td>tier</td>
</tr>
<tr>
<td>16.17</td>
<td>uncompress</td>
</tr>
<tr>
<td>17</td>
<td>Support Commands</td>
</tr>
<tr>
<td>17.1</td>
<td>support</td>
</tr>
<tr>
<td>17.2</td>
<td>debuginfo</td>
</tr>
<tr>
<td>17.3</td>
<td>iostat</td>
</tr>
<tr>
<td>17.4</td>
<td>metasave</td>
</tr>
<tr>
<td>17.5</td>
<td>services</td>
</tr>
<tr>
<td>17.6</td>
<td>thereal</td>
</tr>
<tr>
<td>17.7</td>
<td>top</td>
</tr>
<tr>
<td>17.8</td>
<td>traceroute</td>
</tr>
<tr>
<td>18</td>
<td>System Commands</td>
</tr>
<tr>
<td>18.1</td>
<td>system</td>
</tr>
<tr>
<td>18.2</td>
<td>clock</td>
</tr>
<tr>
<td>18.3</td>
<td>config</td>
</tr>
<tr>
<td>18.4</td>
<td>disable</td>
</tr>
<tr>
<td>18.5</td>
<td>enable</td>
</tr>
<tr>
<td>18.6</td>
<td>status</td>
</tr>
<tr>
<td>18.7</td>
<td>kms</td>
</tr>
<tr>
<td>18.8</td>
<td>license</td>
</tr>
<tr>
<td>18.9</td>
<td>more</td>
</tr>
<tr>
<td>18.10</td>
<td>ntp</td>
</tr>
<tr>
<td>18.11</td>
<td>option</td>
</tr>
<tr>
<td>18.12</td>
<td>stat</td>
</tr>
<tr>
<td>18.13</td>
<td>webservices</td>
</tr>
<tr>
<td>19</td>
<td>Target Commands</td>
</tr>
<tr>
<td>19.1</td>
<td>target</td>
</tr>
<tr>
<td>19.2</td>
<td>iscsi lun</td>
</tr>
<tr>
<td>19.3</td>
<td>iscsi target service</td>
</tr>
<tr>
<td>19.4</td>
<td>iscsi target</td>
</tr>
<tr>
<td>20</td>
<td>Upgrade Commands</td>
</tr>
<tr>
<td>20.1</td>
<td>upgrade</td>
</tr>
<tr>
<td>20.2</td>
<td>get</td>
</tr>
<tr>
<td>20.3</td>
<td>history</td>
</tr>
<tr>
<td>20.4</td>
<td>install</td>
</tr>
<tr>
<td>20.5</td>
<td>repository</td>
</tr>
<tr>
<td>20.6</td>
<td>version</td>
</tr>
</tbody>
</table>
Legal Notice

Last updated: Sep 04, 2017
Document version: 7.3 Rev 0

Copyright © 2017 Veritas Technologies LLC. All rights reserved. Veritas, the Veritas Logo, Veritas InfoScale, and NetBackup are trademarks or registered trademarks of Veritas Technologies LLC or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

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

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

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

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

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

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

https://www.veritas.com/support

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

https://my.veritas.com

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

Worldwide (except Japan) CustomerCare@veritas.com
Japan Customer Care_Japan@veritas.com
1.2 Documentation

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

https://sort.veritas.com/documents
1.3 Documentation feedback

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

doc.feedback@veritas.com

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

http://www.veritas.com/community/
1.4 Veritas Services and Operations Readiness Tools (SORT)

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

2.1 Veritas Access CLI command conventions

This document uses the following conventions when describing commands that are used in the Veritas Access CLI, also sometimes referred to as the CLISH.

2.1.1 Command conventions

- Brackets [] indicate that the enclosed component of the command line is optional.
- Curly braces {} indicate an association between the enclosed options. For example, {opt1 [opt2 ...optn]} means that if the command contains opt1, then the command may optionally contain opt2 ...optn.
- A vertical bar (or the pipe symbol) | separates optional arguments from which you can choose. For example, if a command has the following format, you can choose arg1 or arg2 (but not both):
  command [arg1 | arg2 ]
- Italics indicate that the information is user supplied. For example, the user supplies the pool name, disk, and if the storage pool is isolated or not in the following command:
  Storage> pool create pool_name disk1 [, disk2...] {isolated=[yes|no]}
- An ellipsis (...) means that you can repeat the previous parameter. For example, consider the following command:
  Storage> pool adddisk pool_name disk1 [, disk2,...]
2.2 About accessing the online man pages

You access the online man pages by typing `man name_of_command` at the command line.

The example shows the result of entering the `History> man` command.

**NAME** history - display command history

**SYNOPSIS** history [username] [number_of_lines]

**DESCRIPTION** The `history` command displays the commands executed by the user in the following format: 

```
<time stamp> <status> <message> <command>
```

- `<time stamp>`: MM-DD-YYYY HH:MM
- `<status>`: Success | Error | Warning
- `<message>`: Description of the command.
- `<command>`: Actual command executed by the user

You can also type a question mark (?) at the prompt for a list of all the commands that are available for the command mode that you are in. For example, if you are within the Admin mode, if you type a question mark (?), you see a list of the available commands for the Admin mode.

```
ACCESS> admin ?
Entering admin mode...
ACCESS.Admin>
exit -- Return to the previous menus
logout -- Logout of the current CLI session
man -- Display on-line reference manuals
passwd -- Change the administrator password
show -- Show the administrator details
supportuser -- Enable or disable the support user
user -- Add or delete an administrator
```

To exit the command mode, enter the following command: `exit` To exit the system console, enter the following command: `logout`.

3.1 admin

3.1.1 SYNOPSIS

show [username]
passwd [username]
supportuser disable
supportuser enable
supportuser password
supportuser status
user add username system-admin|storage-admin|master
user delete username

3.1.2 DESCRIPTION

These admin commands are used to display a list of administrators, to add or delete an administrator, and to change the password of an administrator. An administrator can be a Master, System Administrator, or a Storage Administrator. A Master Administrator has all the permissions. Only the Master Administrator can add or delete other administrators.

3.1.3 OPTIONS

show [username]  Show the administrator details of the given username.
passwd [username] Change the password of the given username. Only the Master Administrator can change the password of other administrators.
supportuser disable Disallow non-local logins to support user. Only the Master Administrator can disable the support user. By default, support user is enabled after installation of Veritas Access.
**supportuser enable**  Allow support user to login from anywhere. Only the Master Administrator can enable the support user.

**supportuser password**  Change the password of the support user. Only the Master Administrator can change the password of the support user.

**supportuser status**  Show the status (either enable or disable) of the support user. Only the Master Administrator can see the status of the support user.

**user add username system-admin|storage-admin|master**  Add a new administrator with the given username and privileges.

**user delete username**  Delete an administrator with the given username.

### 3.1.4 EXAMPLES

Display all the administrators on the current system.

```
Admin> show
List of Users
--------
master
```

Display the details of the administrator with username `master`.

```
Admin> show master
Username : master
Privileges : Master
```

Disable the `support` user.

```
Admin> supportuser disable
Disabling support user.
support user disabled.
```

Enable the `support` user.

```
Admin> supportuser enable
Enabling support user.
support user enabled.
```

Display the status of the `support` user.

```
Admin> supportuser status
support user status : Enabled
```

### 3.1.5 SEE ALSO

`user(1), passwd(1), show(1)`
3.2 passwd

3.2.1 SYNOPSIS

passwd [username]

3.2.2 DESCRIPTION

The admin passwd command is used to change the user’s password. Only the Master administrator can change the password of the other administrators. Note: The system does not ask for the old password.

3.2.3 OPTIONS

username  Change the password of the specified user. If username is not specified, the password of the currently logged-in user is changed.

3.2.4 EXAMPLES

Change the password of the currently logged-in user.

Admin> passwd

Change the password of the master user.

Admin> passwd master

3.2.5 SEE ALSO

show(1), user(1)
3.3 show

3.3.1 SYNOPSIS

`show [username]`

3.3.2 DESCRIPTION

The admin `show` command displays the user information that includes the user name and privileges.

3.3.3 OPTIONS

`username` Show details of the specified user. If the `username` is not specified, the command displays a list of all of the users.

3.3.4 EXAMPLES

Display all the administrators on the current system.

```
Admin> show
List of Users
----------
master
```

Display the details of the administrator with username `master`.

```
Admin> show master
Username : master
Privileges : Master
```

3.3.5 SEE ALSO

`user(1), passwd(1)`
3.4 supportuser

3.4.1 SYNOPSIS

supportuser disable
supportuser enable
supportuser password
supportuser status

3.4.2 DESCRIPTION

The supportuser commands disable, enable, and show the status of the support user. The commands are also used to change the password of the support user.

3.4.3 OPTIONS

- **supportuser disable** Disable remote logins to support user. Only the Master Administrator can disable the support user. By default, the support user is enabled after installation of Veritas Access.

- **supportuser enable** Allow the support user to login from anywhere. Only the Master Administrator can enable the support user.

- **supportuser password** Change the password of the support user. Only the Master Administrator can change the password of the support user.

- **supportuser status** Show the status (either enable or disable) of the support user. Only the Master Administrator can see the status of the support user.

3.4.4 EXAMPLES

Disable the support user.

Admin> supportuser disable
Disabling support user.
support user disabled.

Enable the support user.

Admin> supportuser enable
Enabling support user.
support user enabled.

Display the status of the support user.

Admin> supportuser status
support user status : Enabled

3.4.5 SEE ALSO

user(1), passwd(1), show(1)
3.5 user

3.5.1 SYNOPSIS

user add username system-admin|storage-admin|master
user delete username

3.5.2 DESCRIPTION

The admin user commands add or delete a user. A user can be a Master user who has all of the permissions, including adding and deleting users. By default, the password of the new user is the same as the username. A Storage Administrator has access to only storage commands and is responsible for upgrading the cluster and applying the patches. A System Administrator is responsible for configuring the NFS server and exporting the file system, adding or deleting new nodes to the cluster, and configuring other network parameters like DNS, NIS, and so on.

3.5.3 OPTIONS

user add username system-admin|storage-admin|master Add a user with specific privileges.
user delete username Delete the specified user from the current system.

3.5.4 EXAMPLES

Add a Master with username master1.

Admin> user add master1 Master

Add a System Administrator with username admin.

Admin> user add admin System-admin

Delete a user with username admin.

Admin> user delete admin

3.5.5 SEE ALSO

show(1)
4.1 backup

4.1.1 SYNOPSIS

netbackup master-server server
netbackup emm-server server
netbackup media-server add server
netbackup media-server delete server
netbackup sanclient enable|disable
netbackup exclude_list show [policy] [schedule]
netbackup exclude_list add pattern [policy] [schedule]
netbackup exclude_list delete pattern [policy] [schedule]
netbackup include_list show [policy] [schedule]
netbackup include_list add pattern [policy] [schedule]
netbackup include_list delete pattern [policy] [schedule]
install version [url]
uninstall
virtual-ip ipaddr [device]
virtual-name name
show
status
start [nodename]
stop
4.1.2 DESCRIPTION

The backup commands configure the built-in NetBackup client software.

4.1.3 NetBackup Client

Each node in the cluster includes built-in NetBackup client software of version 7.7 for users with the NetBackup data protection suite. The NetBackup Master Server and NetBackup Media Server should be 7.7 or higher.

NetBackup installed on the cluster nodes works as a NetBackup standard client to perform IP-based backups and a NetBackup SAN client to perform SAN-based backups of file systems.

The backup netbackup commands configure the local NetBackup installation to work with an external NetBackup Master Server.

The backup virtual-name command configures a NetBackup installation on the cluster nodes to use name as its hostname.

The backup netbackup master-server, netbackup emm-server, and netbackup media-server commands configure the NetBackup client to work with the given NetBackup installation.

The backup virtual-ip command configures the built-in NetBackup Client installation to use ipaddr as its virtual IP address and device as the network interface for the virtual ip.

The backup install command installs a one higher or one lower supported version of the Netbackup client.

The backup uninstall command uninstalls the currently installed version of the Netbackup Client.

Note: The NetBackup SAN client should only be enabled if the required licenses are installed on the NetBackup Master Server. If the required licenses for the NetBackup SAN client are not available on the NetBackup Master Server, then the backup service fails to start. If you do not have the required license for the NetBackup SAN client, then you must disable the SAN client using netbackup sanclient disable. Otherwise, the backup service fails to start.

The built-in NetBackup client software also supports snapshot-based backups. To use snapshot-based backups with the built-in NetBackup client, use snapshot type as VxFS_Checkpoint in the NetBackup policy configuration.

4.1.4 OPTIONS

- **server** Hostname of the server to use as the NetBackup Master Server, EMM Server, or Media Server. Make sure that server can be resolved through DNS and its IP address can be resolved back to server through the DNS reverse lookup.

- **ipaddr** Virtual IP address to be used by the NetBackup installation on Veritas Access nodes. Make sure that ipaddr can be resolved back to the hostname configured through the backup virtual-name command for proper functioning of NetBackup.

- **name** Hostname to be used by a NetBackup installation on the Veritus Access nodes. Make sure that name can be resolved through DNS and its IP address can be resolved back to name through a DNS reverse lookup. Also make sure that name resolves to the IP address configured through the backup virtual-ip command.

- **version** Netbackup client version to be installed. Netbackup versions 7.7 and 7.6 are currently supported.

- **url** URL specifying the location of the Netbackup client to be installed. Currently, supported protocols are http, ftp, and scp.
virtual-ip ipaddr [device] Configure the NetBackup installation on the Veritas Access nodes to use ipaddr as its highly available virtual IP address and device as the network interface for the virtual IP address.

To remove the virtual IP address configured for backup, use “-” for ipaddr. Like, “virtual-ip -”. A network mask can be provided with the IP address as the prefix length for the ipaddr. For example, virtual-ip 10.209.107.151/22.

IPv6 addresses can be specified as “virtual-ip fec0::20c:29ff:fe8e:2203/64”.

virtual-name name Configure a NetBackup installation on Veritas Access nodes to use name as its hostname. Make sure that name resolves to the IP address that is configured using the virtual-ip command.

netbackup master-server server Configure the hostname of the NetBackup Master Server name to be used by the built-in NetBackup client installation. This setting is mandatory, if the NetBackup client software needs to be used. Make sure that the server hostname can be resolved through DNS, and its IP address can be resolved back to server hostname through the DNS reverse lookup.

netbackup emm-server server Configure an external NetBackup EMM Server name to be used by the NetBackup installation on the Veritas Access nodes. This setting is mandatory, if the NetBackup client software needs to be used. Make sure that the server hostname can be resolved through DNS, and its IP address can be resolved back to server hostname through the DNS reverse lookup.

netbackup media-server add server Add an external NetBackup Media Server name to be used by the NetBackup installation on the Veritas Access nodes. This setting is optional, since if the Media Server name is not added, the local NetBackup client installation uses the NetBackup Master Server as the NetBackup Media Server. Make sure that the server hostname can be resolved through DNS, and its IP address can be resolved back to server hostname through the DNS reverse lookup.

.netbackup media-server delete server .fi Delete an already configured NetBackup Media Server name.

netbackup sanclient enable|disable Enable or disable the NetBackup SAN client. The NetBackup SAN client should only be enabled if the required licenses are installed on the NetBackup Master Server. If the required licenses for the NetBackup SAN client are not available on the NetBackup Master Server, then the backup service fails to start.

netbackup exclude_list show [policy] [schedule] Show the entries in the exclude list entries. Exclude entries can also be explicitly listed for a specific policy by using the policy attribute. If schedule is specified, then the exclude list entries for the policy specified in policy and schedule schedule are shown.

netbackup exclude_list add pattern [policy] [schedule] Add the given pattern to the list of files to be excluded. File names matching pattern are excluded from backups. If policy, then the pattern is only applicable for backups of the specific policy.

netbackup exclude_list delete pattern [policy] [schedule] Delete the given pattern from the list of patterns to be excluded.

netbackup include_list show [policy] [schedule] Show the entries in the include list entries. Include entries can also be explicitly listed for a specific policy by using the policy attribute. If schedule is specified, then include list entries for the policy specified in policy and schedule schedule are shown.

netbackup include_list add pattern [policy] [schedule] Add the given pattern to the list of files to be included. File names matching pattern are always included in backups. If policy, then the pattern is only applicable for backups of the specific policy.
netbackup include_list delete pattern [policy] [schedule] Delete the given pattern from the list of patterns to be included.

install version [url] The backup install command installs a one higher or one lower supported version of the NetBackup client.

uninstall The backup uninstall command uninstalls the currently installed version of the NetBackup client.

show This command shows the configured settings.

status Display the status of the current backup activities.

start [nodename] Start processes that handle backup and restore. Also online a virtual IP address.

stop Stop processes that handle backup and restore. Also offline a virtual IP address.

### 4.1.5 EXAMPLES

Add an external NetBackup Master Server.
```
Backup> netbackup master-server nbumaster.veritas.com
Success.
```

Add an external NetBackup EMM Server name (which can be the same as the NetBackup Master Server).
```
Backup> netbackup emm-server nbumaster.veritas.com
Success.
```

Add an external NetBackup Media Server name (if the NetBackup Media Server is not co-located with the NetBackup Master Server).
```
Backup> netbackup media-server add nbumedia.veritas.com
Success.
```

Delete an already added external Media Server name.
```
Backup> netbackup media-server delete nbumedia.veritas.com
Success.
```

Configure or change the virtual IP address and network interface of the NetBackup client on the Veritas Access nodes.
```
Backup> virtual-ip 10.10.10.10 pubeth1
Success.
```

Enable the NetBackup SAN client.
```
Backup> netbackup sanclient enable
Success.
```

Configure or change the hostname of the NetBackup installation on the Veritas Access nodes.
```
Backup> virtual-name nbuclient.veritas.com
Success.
```

Install Netbackup Client 7.7 using a Netbackup client tar with SCP.
Install NetBackup client 7.7 using a NetBackup client tar with FTP.

```
Backup> install 7.7 scp://root@10.209.106.59:/home/NetBackup_7.7.3_CLIENTS2.tar.gz
Copying from scp://root@10.209.106.59:/home/NetBackup_7.7.3_CLIENTS2.tar.gz
Password:
Copying from scp://root@10.209.106.59:/home/NetBackup_7.7.3_CLIENTS2.tar.gz completed
100% [#] NBU Client Installation completed
```

Install NetBackup client 7.7 using a NetBackup client tar with HTTP.

```
Backup> install 7.7 ftp://ftp@10.209.106.59:/NetBackup_7.7.3_CLIENTS2.tar.gz
Copying from ftp://ftp@10.209.106.59:/NetBackup_7.7.3_CLIENTS2.tar.gz
Password:
Copying from ftp://ftp@10.209.106.59:/NetBackup_7.7.3_CLIENTS2.tar.gz completed
100% [#] NBU Client Installation completed
```

Uninstall the currently installed NetBackup client.

```
Backup> uninstall
100% [#] NBU Client uninstallation completed
```

Show the configured settings.

```
Backup> show
Virtual Name: nbuclient.veritas.com
Virtual IP: 10.10.10.10/24
NetBackup Master Server: nbumaster.veritas.com
NetBackup EMM Server: nbumaster.veritas.com
NetBackup Media Server(s): not configured
Backup Device: pubeth1
```

Display the status when no backup jobs are running.

```
Backup> status
Virtual IP state : up
Backup service online node : node_01
NetBackup Client state : running
NetBackup SAN Client state : running
No backup/restore jobs running.
```

Display the status when backup jobs are running that involve file systems using the NetBackup client.

```
Backup> status
Virtual IP state : up
Backup service online node : node_01
NetBackup Client state : working
NetBackup SAN Client state : running
Some filesystems are busy in backup/restore jobs by NetBackup Client
```

4.1. backup
Start processes that handle backup and restore.

```
Backup> start
NetBackup Client started successfully.
Success.
```

Stop processes that handle backup and restore when backup jobs are running.

```
Backup> stop
ACCESS backup ERROR V-288-0 Cannot stop, some backup jobs are running.
```

### 4.1.6 SEE ALSO

netbackup(1), virtual-ip(1), virtual-name(1), show(1), status(1), start(1), stop(1), install(1), uninstall(1)
4.2 install

4.2.1 SYNOPSIS

install version [url]

4.2.2 DESCRIPTION

The backup install command installs a one higher or one lower supported version of the NetBackup client. Each node in the cluster includes built-in NetBackup client software of version 8.0 for users with the NetBackup data protection suite.

4.2.3 OPTIONS

version  NetBackup client version to be installed. NetBackup versions 8.0 and 7.7 are currently supported.

url  URL specifying the location of the NetBackup client to be installed. Currently, supported protocols are http, ftp, and scp.

4.2.4 EXAMPLES

Install the NetBackup client 7.7 using a NetBackup client tar with SCP.

```
Backup> install 7.7 scp://root@10.209.106.59:/home/NetBackup_7.7.1_CLIENTS2.tar.gz
Copying from scp://root@10.209.106.59:/home/NetBackup_7.7.1_CLIENTS2.tar.gz
Password:
Copying from scp://root@10.209.106.59:/home/NetBackup_7.7.1_CLIENTS2.tar.gz completed
100% [#] NBU Client Installation completed
```

4.2.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), show(1), status(1), stop(1), install(1), uninstall(1)
4.3 netbackup

4.3.1 SYNOPSIS

netbackup master-server set server
netbackup master-server reset
netbackup emm-server set server
netbackup emm-server reset
netbackup media-server add server
netbackup media-server delete server
netbackup sanclient enable|disable
netbackup exclude_list show [policy] [schedule]
netbackup exclude_list add pattern [policy] [schedule]
netbackup exclude_list delete pattern [policy] [schedule]
netbackup include_list show [policy] [schedule]
netbackup include_list add pattern [policy] [schedule]
netbackup include_list delete pattern [policy] [schedule]

4.3.2 DESCRIPTION

Each node in the cluster includes built-in NetBackup client software of version 7.7 for users with the NetBackup data protection suite. The NetBackup Master server and NetBackup Media Server should be 7.7 or higher. See the Veritas Access Installation Guide for the supported NetBackup versions.

NetBackup installed on the cluster nodes works as a NetBackup standard client to perform IP-based backups. The NetBackup SAN client performs SAN-based backups of file systems.

The backup netbackup commands configure the local NetBackup installation with an external NetBackup Master Server.

The backup virtual-name command configures a NetBackup installation on cluster nodes to use name as its hostname.

The backup netbackup master-server, netbackup emm-server, and netbackup media-server configures the NetBackup client to work with the given NetBackup installation.

The backup virtual-ip command configures the built-in NetBackup client to use ipaddr as its virtual IP address and device as the network interface for the virtual IP.

Note: The NetBackup SAN client should only be enabled if the required licenses are installed on the NetBackup Master Server. If the required licenses for the NetBackup SAN client are not available on the NetBackup Master Server, then the backup service fails to start. If you do not have the required license for the NetBackup SAN client, then you must disable the SAN client using netbackup sanclient disable. Otherwise, the backup service fails to start.

The built-in NetBackup client software also supports snapshot-based backups. To use snapshot-based backups with the built-in NetBackup client, use snapshot type as VxFS_Checkpoint in the NetBackup policy configuration.
4.3.3 OPTIONS

**server** Hostname of the server to use as the NetBackup Master Server, EMM Server, or Media Server. Make sure that `server` can be resolved through DNS and its IP address can be resolved back to `server` through the DNS reverse lookup.

**netbackup master-server set server** Configure the hostname of the NetBackup Master Server name to be used by the built-in NetBackup client installation. This setting is mandatory if the NetBackup client software needs to be used. Make sure that the `server` hostname can be resolved through DNS, and its IP address can be resolved back to `server` hostname through the DNS reverse lookup.

**netbackup emm-server set server** Configure an external NetBackup EMM Server name to be used by the NetBackup installation on the Veritas Access nodes. This setting is mandatory, if the NetBackup client software needs to be used. Make sure that the `server` hostname can be resolved through the DNS, and its IP address can be resolved back to `server` hostname through the DNS reverse lookup.

**netbackup media-server add server** Add an external NetBackup Media Server name to be used by the NetBackup installation on the Veritas Access nodes. This setting is optional, since if the Media Server name is not added, the local NetBackup client installation uses the NetBackup Master Server as the NetBackup Media Server. Make sure that the `server` hostname can be resolved through DNS, and its IP address can be resolved back to `server` hostname through the DNS reverse lookup.

**netbackup media-server delete server** Delete an already configured NetBackup Media Server name.

**netbackup sanclient enable|disable** Enable or disable the NetBackup SAN client. The NetBackup SAN client should only be enabled if the required licenses are installed on the NetBackup Master Server. If the required licenses for the NetBackup SAN client are not available on the NetBackup Master Server, then the backup service fails to start.

**netbackup exclude_list show [policy] [schedule]** Show the entries in the exclude list entries. Exclude entries can also be explicitly listed for a specific policy by using the `policy` attribute. If `schedule` is specified, then exclude list entries for the policy specified in `policy` and schedule `schedule` are shown.

**netbackup exclude_list add pattern [policy] [schedule]** Add the given pattern to the list of files to be excluded. File names matching `pattern` are excluded from backups. If `policy` is used, then the `pattern` is only applicable for backups of the specific policy.

**netbackup exclude_list delete pattern [policy] [schedule]** Delete the given pattern from the list of patterns to be excluded.

**netbackup include_list show [policy] [schedule]** Show the entries in the include list entries. Include entries can also be explicitly listed for a specific policy by using the `policy` attribute. If `schedule` is specified, then include list entries for the policy specified in `policy` and schedule `schedule` are shown.

**netbackup include_list add pattern [policy] [schedule]** Add the given pattern to the list of files to be included. File names matching `pattern` are always included in backups. If `policy` is used, then the `pattern` is only applicable for backups of the specific policy.

**netbackup include_list delete pattern [policy] [schedule]** Delete the given pattern from the list of patterns to be included.

4.3.4 EXAMPLES

Add an external NetBackup Master Server.
Backup> netbackup master-server set nbmaster.veritas.com
Success.

Add an external NetBackup EMM Server name (which can be the same as the NetBackup Master Server).

Backup> netbackup emm-server set nbmaster.veritas.com
Success.

Add an external NetBackup Media Server name (if the NetBackup Media Server is not co-located with the NetBackup Master Server).

Backup> netbackup media-server add nbmedia.veritas.com
Success.

Delete an already added external Media Server name.

Backup> netbackup media-server delete nbmedia.veritas.com
Success.

Enable the NetBackup SAN client.

Backup> netbackup sanclient enable
Success.

Show the exclude list entries.

Backup> netbackup exclude_list show
Pattern Policy Schedule
------- ------ --------
hosts - -
iscsid.conf - -
iscsid.conf NBU_nasgw12 -
/vx/fs100/as* policy -
/vx/fs100/*mp3 policy -
/vx/fs200/bs* policy2 sched3

Add an entry to the include list for policy with name backup_policy3.

Backup> netbackup include_list add *.jpg backup_policy3
Success.

4.3.5 SEE ALSO

backup(1), virtual-ip(1), virtual-name(1), show(1), status(1), start(1), stop(1)
4.4 show

4.4.1 SYNOPSIS

show

4.4.2 DESCRIPTION

The backup show command displays the configured settings. The displayed settings may not be currently used by the Veritas Access nodes. When some settings are configured, there might be backup and restore jobs that are running, and so those settings do not immediately take effect. To fill this gap, you have to use the backup stop command followed by the backup start command.

4.4.3 OPTIONS

show

This command shows the configured settings.

4.4.4 EXAMPLES

Show the configured settings.

```
Backup> show
Virtual Name: nbuclient.veritas.com
Virtual IP: 10.10.10.10/24
NetBackup Master Server: nbumarster.veritas.com
NetBackup EMM Server: nbumarster.veritas.com
NetBackup Media Server(s): not configured
Backup Device: pubethl
NetBackup Client Version: 8.0
NetBackup global log level: not configured
NetBackup database log level: not configured
Enable robust logging: not configured
Enable critical process logging: not configured
```

4.4.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), status(1), start(1), stop(1)
4.5 start

4.5.1 SYNOPSIS

start [nodename]

4.5.2 DESCRIPTION

The backup start command starts backup processes that handle backup and restore. It will do nothing if those processes are currently running. It places the virtual IP address configured through the backup virtual-ip command in online mode on any of the currently active nodes or nodename if specified.

4.5.3 OPTIONS

start

Start processes that handle backup and restore. Also places the virtual IP address in online mode.

4.5.4 EXAMPLES

Start processes that handle backup and restore.

```
Backup> start
NetBackup Client started successfully.
```

4.5.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), show(1), status(1), stop(1)
4.6 status

4.6.1 SYNOPSIS

status

4.6.2 DESCRIPTION

The backup status command shows if the NetBackup client has started or stopped on the Veritas Access nodes. If the NetBackup client has currently started and is running, it also shows if there are any ongoing backup or restore jobs.

4.6.3 OPTIONS

status

Display the status of current backup activities.

4.6.4 EXAMPLES

Display the status when no backup jobs are running.

```
Backup> status
Virtual IP state : up
Backup service online node : node_01
NetBackup client state : online
NetBackup SAN client state : online

No backup or restore jobs running.
```

Display the status when backup jobs are running that involve file systems using the NetBackup client.

```
Backup> status
Virtual IP state : up
Backup service online node : node_01
NetBackup client state : online
NetBackup SAN client state : online

Some file systems are busy performing backup or restore jobs by the NetBackup client
```

4.6.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), show(1), start(1), stop(1)
4.7 stop

4.7.1 SYNOPSIS

stop

4.7.2 DESCRIPTION

The backup stop command stops processes that handle backup and restore. Nothing stops if there are any backup jobs running that involve file systems on the Veritas Access nodes. It will also offline the virtual IP address configured by using the backup virtual-ip command.

4.7.3 OPTIONS

stop

Stop processes that handle backup and restore. It also places the virtual IP address in the offline mode.

4.7.4 EXAMPLES

Stop processes that handle backup and restore when backup jobs are running.

```
Backup> stop
ACCESS backup ERROR V-288-0 Cannot stop, some backup jobs are running.
```

4.7.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), show(1), status(1), start(1)
4.8 uninstall

4.8.1 SYNOPSIS

uninstall

4.8.2 DESCRIPTION

The backup uninstall command uninstalls the currently installed version of the Netbackup client.

4.8.3 EXAMPLES

Uninstall the currently installed Netbackup client.

```
Backup> uninstall
100% [#] NBU Client uninstallation completed
```

4.8.4 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), virtual-name(1), show(1), status(1), stop(1), install(1), uninstall(1)
4.9 virtual-ip

4.9.1 SYNOPSIS

virtual-ip set ipaddr [device]
virtual-ip reset

4.9.2 DESCRIPTION

The backup virtual-ip command configures the built-in NetBackup client to use ipaddr as its virtual IP address and device as the network interface for the virtual IP.

4.9.3 OPTIONS

ipaddr Virtual IP address to be used by the NetBackup client on the Veritas Access nodes. Make sure that ipaddr can be resolved back to the hostname, configured by using the backup virtual-name command.

virtual-ip set ipaddr [device] Configure the NetBackup client on the Veritas Access nodes to use ipaddr as its highly available virtual IP address and device as the network interface for the virtual IP address.

A network mask can be provided with the IP address as the prefix length for the ipaddr. For example, virtual-ip set 10.209.107.151/22.

IPv6 addresses can be specified as virtual-ip set fec0::20c:29ff:fe8e:2203/64.

4.9.4 EXAMPLES

Configure or change the virtual IP address of the NetBackup client on the Veritas Access nodes.

Backup> virtual-ip set 10.10.10.10/20 pubeth1
Success.

Reset the virtual IP address configured for backup.

Backup> virtual-ip reset
Success.

To configure an IPv6 address for backup.

Backup> virtual-ip set fec0::20c:29ff:fe8e:2203/64 pubeth0
Success.

4.9.5 SEE ALSO

backup(1), netbackup(1), virtual-name(1), show(1), status(1), start(1), stop(1)
4.10 virtual-name

4.10.1 SYNOPSIS

    virtual-name set name
    virtual-name reset

4.10.2 DESCRIPTION

The backup virtual-name command configures the NetBackup client installation on the Veritas Access nodes to use name as its hostname.

4.10.3 OPTIONS

    name  Hostname to be used by a NetBackup client installation on the Veritas Access nodes. Make sure that name can be resolved through DNS and its IP address can be resolved back to name through a DNS reverse lookup. Also make sure that name resolves to the IP address configured through the backup virtual-ip command.

    virtual-name set name  Configure a NetBackup client installation on the Veritas Access nodes to use name as its hostname. Make sure that name resolves to the IP address that is configured using the virtual-ip command.

4.10.4 EXAMPLES

Configure or reset the hostname of the NetBackup client installation on the Veritas Access nodes.

Backup> virtual-name set nbuclient.veritas.com
Success.

Backup> virtual-name reset
Success.

4.10.5 SEE ALSO

backup(1), netbackup(1), virtual-ip(1), show(1), status(1), start(1), stop(1)
5.1 cifs

5.1.1 SYNOPSIS

server start|stop|status
share add filesystem sharename [@virtual_ip] [cifsoptions]
share modify sharename [@virtual_ip] [cifsoptions]
share delete sharename [@virtual_ip]
share show [sharename]
share allow sharename @group1 [, @group2, user1, user2, ...]
share deny sharename @group1 [, @group2, user1, user2, ...]
set domaincontroller servernames
set domainuser username
set domain domainname
set workgroup workgroup
set allow_trusted_domains yes|no [trusted_domains]
set ntlm_auth yes|no
set security ad|sluser
set idmap_backend ldap [idmap_ou] [uid_range]
set idmap_backend rid [uid_range]
set idmap_backend hash
set idmap_backend ad [uid_range]
set homedirfs [filesystemlist] [full_acl]
set aio_size size
set data_migration yes|no
set clustering_mode normal|ctdb
local user add username [grouplist]
local password username
local user delete username
local user show [username]
local group add groupname
local group delete groupname
local group show [groupname]
local user members username grouplist
mapuser add CIFSusername domainname NFSusername
mapuser remove CIFSusername [domainname]
mapuser show [CIFSusername] [domainname]
homedir set username [domainname] [fs_name]
homedir delete username [domainname]
homedir deleteall
homedir show [username] [domainname]
show

5.1.2 DESCRIPTION

The cifs commands maintain the current table of exported file systems for CIFS.

For the CIFS service to work properly in an active directory domain environment, the following protocols and firewall ports need be allowed or opened in the environment to allow the CIFS server to communicate smoothly with the active directory domain controller(s) and Windows CIFS clients.

ICMP: Internet Control Message Protocol (ICMP) protocol must be allowed through the firewall from the CIFS server to the domain controllers. Enable “Allow incoming echo request” is a must requirement for running the CIFS service.

Other ports and protocols:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP and UDP 53</td>
<td>DNS</td>
</tr>
<tr>
<td>TCP and UDP 88</td>
<td>Kerberos</td>
</tr>
<tr>
<td>TCP 139</td>
<td>DFSN, NetBIOS Session Service, NetLog</td>
</tr>
<tr>
<td>TCP and UDP 445</td>
<td>SMB,CIFS,DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc</td>
</tr>
<tr>
<td>TCP and UDP 464</td>
<td>Kerberos change/set password</td>
</tr>
<tr>
<td>TCP 3268</td>
<td>LDAP GC</td>
</tr>
</tbody>
</table>

If LDAP with SSL is required, the following ports need to be opened:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP 636</td>
<td>LDAP SSL</td>
</tr>
<tr>
<td>TCP 3269</td>
<td>LDAP GC SSL</td>
</tr>
</tbody>
</table>
5.1.3 OPTIONS

**cifsoptions** Comma-separated list of export options for a CIFS share are: ro, rw, guest, noguest, oplocks, nooplocks, full_acl, no_full_acl, enable_encryption, disable_encryption, shadow_copy, hide_unreadable, veto_sys_files, enable_durable_handles, owner=ownername, group=groupname, fs_mode=fspermission, dir_mask=dirpermission, create_mask=filepermission, allow=userid+@group, deny=userid+@group, max_connections=connections. The default export options are: ro, noguest, oplocks, no_full_acl, fs_mode=1777, dir_mask=775, create_mask=775, allow=all.

**server start|stop|status** Start, stop, or display the status of the CIFS resources. All variable settings made using the set command come into effect only when the server is restarted. For example, set can be used to set the security to ads or to a value other than ads, but the server joins or leaves the Active Directory domain only when the server is restarted after using the set command. One exception is the case when the server is already stopped, and later security is set to a value other than ads.

**share add filesystem sharename [@virtual_ip] [cifsoptions]** Export the file system with the given sharename. The new options are updated after the command is run. In ctdb clustering mode, you can give the directory path instead of the file system. While specifying the directory path, make sure it always starts with the file system name (Note: not with the mount point /vx). If @virtual_ip is specified, the share can only be accessed by virtual_ip.

**share modify sharename [@virtual_ip] [cifsoptions]** Re-export the file system with the given sharename. The new options are updated after the command is run. In ctdb clustering mode, you can give the directory path instead of the file system. While specifying the directory path, make sure it always starts with the file system name (Note: not with the mount point /vx). If @virtual_ip is specified, the share can only be accessed by virtual_ip.

**share delete sharename** Unexport the share with the name sharename.

**share show [sharename]** List all the exported resources. If sharename is specified, then Veritas Access prints all the details of the given sharename.

**share allow sharename @group1 [@group2,user1,user2,...]** Allow only the specified users and groups to access the share. If all is specified, then default access restrictions are restored on the share. User or group separator can be a comma or a plus symbol, double backslash should be added between domain name and user or group in case the allowed one comes from the trusted domain.

**share deny sharename @group1 [@group2,user1,user2,...]** Deny the specified users and groups to access the share. If all is specified, then all the users and groups are not able to access the share. User or group separator can be a comma or a plus symbol, double backslash should be added between domain name and user or group in case the denied one comes from the trusted domain.

**set domaincontroller servernames** Set the comma-separated list of domain controller server names. A domain controller can either be an Active Directory server or a Windows NT 4.0 domain controller.

**set domainuser username** Set the name of the domain-user. This username is used for authentication for the domain join operation.

**set domain domainname** Set the domain name. This also sets the WORKGROUP of the system.

**set workgroup workgroup** Set the workgroup name. If name of the WORKGROUP or NetBIOS domain name is different from the domain name, use this command to set the workgroup name.

**set allow_trusted_domains yes|no [trusted_domains]** If allow_trusted_domains is set to yes, then multiple domain environments are allowed. Otherwise multiple domain environments are not allowed. Note: This option cannot be set to yes if security mode is user. User can also specify the trusted domains that allow access to the CIFS server when this option is set to yes and the idmap
backend is set to **rid** or **ad**. By default, all the trusted domains are included in the configuration. Default allow_trusted_domains value: **no**

**set ntlm_auth yes|no** If ntlm_auth is set to no, then an NTLMv2 response needs to be sent by the client. Otherwise Veritas Access attempts to authenticate users using the NTLM-encrypted password response. Default ntlm_auth value: **yes**

**set security ads|user** Set CIFS security to user (user-level security that a client must log on with a valid username and password), or ads (CIFS server acts as a domain member in an Active Directory). Before setting the security to ads, it is required to set domain, domaincontroller, and domainuser. When the user executes the server start command, CIFS server asks for the password corresponding to the domainuser to join in the AD. If using security as ads, make sure that the clock of the AD server and the CIFS server is set to the same time. Use the NTP server if possible. Default security Value: **user**

**set idmap_backend ldap [idmap_ou] [uid_range]** This option tells the CIFS server to obtain SID to UID/GID mappings from a common LDAP backend. The LDAP server used for this has to be configured through the ILDAP sub-section in the network section. Trusted domains are allowed if allow_trusted_domains is set to yes. The idmap_ou is optional and set to cifsidmap. By default, the user can specify if the CIFS idmap OrganizationalUnitName(OU) is named differently on the LDAP server. The uid_range is optional and set to 10000-1000000 by default.

**set idmap_backend rid [uid_range]** User can use this option to get the unique SID to UID/GID mappings based on RID and LOW_RANGE_ID. Trusted domains are allowed if allow_trusted_domains is set to yes. The uid_range is set to 10000-1000000 by default. Change it in case there are more than 1,000,000 users existing on the local cluster, joined active directory, or trusted domains. Note: Do not attempt to modify LOW_RANGE_ID(10000) if there is user data on the CIFS server, it may lead to data access denied for the UID changes.

**set idmap_backend hash** User can use this option to get the unique SID to UID/GID mappings by the implemented hashing algorithm. Trusted domains are allowed if allow_trusted_domains is set to yes.

**set idmap_backend ad [uid_range]** User can use this option to get the unique UID/GID from the domain by reading id mappings from an AD server that uses RFC2307/SFU schema extensions, this is a readonly idmap backend. Trusted domains are allowed if allow_trusted_domains is set to yes. A valid user from a domain or a trusted domain should have a UID as well as a GID for the user’s primary group. The uid_range is set to 10000-1000000 by default, change it in case there are more than 1,000,000 users existing on the local cluster, joined active directory, or trusted domains. Note: ID range is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

**set homedirfs [filesystemlist] [full_acl]** Set the given list of file systems to be used for the home directory. All of the home directories of the users are created in these file systems. filesystem is a comma-separated list of file system names. full_acl can be set as an option. Automatic migration of the content of users (i.e., users home directories) from one file system to another file system while switching homedir is not supported. So if an administrator changes homedir from fs1 to fs2, then home directories of the user do not migrate from fs1 to fs2 automatically.

**set aio_size size** Set aio_fork option. If size is not 0, then enable aio_fork and set it as aio read/write size. If it’s 0, then disable aio_fork and set 0 to aio read/write size.

**set data_migration yes|no** User can use this option to enable data migration from a Windows machine by a domain administrator when ACL information for files or directories should be preserved. The ROBOCOPY command from the Windows Resource Kit Tools is required to complete the task. Set the option to yes and restart the CIFS server, and then data migration mode is enabled. Set the option to no after data migration is completed for CIFS server security.
**set clustering_mode normal|ctdb** Set clustering mode for the CIFS server. There are two clustering modes available with Veritas Access: normal and ctdb. Each clustering mode supports all of the three operating modes. The CTDB clustering mode is a different clustered implementation of Veritas Access CIFS, which supports all the features that are supported by normal clustering mode as well as some additional features. Veritas Access supports automated and seamless migration of shares and home directories from one mode to another.

**local user add username [grouplist]** Add the local CIFS user. This user gets authenticated when security is set to user.

**local password username** Reset the password for the local CIFS user.

**local user delete username** Delete the specified CIFS user.

**local user show [username]** Show UID and group(s) details of the given username.

**local group add groupname** Add the local CIFS group.

**local group delete groupname** Delete the local CIFS group.

**local group show [groupname]** Show the list of available local CIFS groups. If ‘groupname’ is specified, it shows all the users belonging to that group.

**local user members username grouplist** Add the local CIFS user to the given groups in the grouplist.

**mapuser add CIFSUsername domainname NFSUsername** Map CIFS user to NFS user. This mapping is useful when the same file system is accessed using both CIFS and NFS. This functionality can also be used to map multiple users to a single username to share common data.

**mapuser remove CIFSUsername [domainname]** Remove the mapping between CIFS and NFS user. It may be possible that the CIFS user may not be able to access its previous data after removing the mapping. Default domain is local.

**mapuser show [CIFSUsername] [domainname]** Show the mapping between CIFS and NFS user. If CIFS Username is not specified, it shows all the existing mappings. Default domain name is local.

**homedir set username [domainname] [fs_name]** Set the homedir for the given user. If the home directory does not exist for the given user, this command creates that user’s home directory. Use fs_name to specify the home directory file system where the user’s home directory is created. Otherwise, the user’s home directory is created on the home directory file system that has the fewest home directories. Use storage quota cifshomedir set to set the quota vaule for the user, otherwise the value set from the storage quota cifshomedir setdefault is used to configure the quota limit. If either user or default quota is not set, 0 is taken as the default value that is treated as the unlimited quota.

**homedir delete username [domainname]** Delete the home directory of the given user.

**homedir deleteall** Delete all of the home directories on the homedir file system.

**homedir show [username] [domainname]** Display homedir usage information.

**show** Display the list of all the global options and their values. Use the set command to modify these values.

### 5.1.4 EXAMPLES

Add a local CIFS group grp1
Create the new CIFS user `usr1` and assign it to existing groups `grp1`.

```
CIFS> local user add usr1 grp1
Input password for usr1.
Enter password:
Re-enter password:
Adding USER : usr1
Success: User usr1 created successfully
```

Reset password for the local CIFS user `usr1`.

```
CIFS> local password usr1
Changing password for usr1.
New password:
Re-enter new password:
Password changed for user: 'usr1'
```

Delete the local CIFS user `usr1`.

```
CIFS> local user delete usr1
Deleting User: usr1
Success: User usr1 deleted successfully
```

Map CIFS user to NFS user.

```
CIFS> mapuser add administrator VERITASDOMAIN.COM nfsusr1
```

Remove the mapping between CIFS and NFS user.

```
CIFS> mapuser remove administrator VERITASDOMAIN.COM
```

Show the mapping between CIFS and NFS user.

```
CIFS> mapuser show administrator VERITASDOMAIN.COM
CIFSUserName DomainName NFSUserName
administrator VERITASDOMAIN nfsusr1
```

Export the file system `fs1` with name `share1`.

```
CIFS> share add fs1 share1
Exporting CIFS filesystem : share1 ...
```

Display the list of shares exported over CIFS.

```
CIFS> share show
```
Veritas Access Command Reference Guide Documentation, Release 7.3

CIFS> share show

<table>
<thead>
<tr>
<th>ShareName</th>
<th>FileSystem</th>
<th>ShareOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>share1</td>
<td>fs1</td>
<td>owner=root,group=root</td>
</tr>
</tbody>
</table>

Unexport the share with the name share1:

CIFS> share delete share1
Unexporting CIFS share : share1 ....

Allow user user1 and group group1 to access the share share1:

CIFS> share allow share1 user1,@group1
Warning: Modifying an already existing share. ..........Done

Allow trusted domain user user1 and group group1 to access the share share1:

CIFS> share allow share1 domain\\\\user1,@domain\\\\group1
Warning: Modifying an already existing share. ..........Done

Deny user user1 and group group1 to access the share share1:

CIFS> share deny share1 user1,@group1
Warning: Modifying an already existing share. ..........Done

Deny trusted domain user user1 and group group1 to access the share share1:

CIFS> share deny share1 domain\\\\user1,@domain\\\\group1
Warning: Modifying an already existing share. ..........Done

Setting the domain parameters for joining an active directory or NT domain. In this example, the name of the domain is set to VERITASDOMAIN.COM, domain user is set to administrator, and domain controller for the domain VERITASDOMAIN.COM is set to VERITASSERVER:

CIFS> set domain `\VERITASDOMAIN.COM`
Global option updated. Note: Restart the CIFS server.
CIFS> set domainuser `\administrator`
Global option updated. Note: Restart the CIFS server.
CIFS> set domaincontroller `\VERITASSERVER`
Global option updated. Note: Restart the CIFS server.

After setting all of the above domain parameters, the user can set the security to either ads if the domain controller is an active directory server, or the user can set the security to domain if the domain controller is an NT domain controller:

CIFS> set security `\ads`
Global option updated. Note: Restart the CIFS server.

Display the list of global options:

CIFS> show

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>----</td>
<td>-----</td>
</tr>
<tr>
<td>netbios name test</td>
<td></td>
</tr>
</tbody>
</table>

5.1. cifs
ntlm auth yes
allow trusted domains no
homedirfs
aio size 0
idmap backend rid:10000-1000000
workgroup VERITASDOMAIN
security ads
Domain VERITASDOMAIN.COM
Domain user administrator
Domain Controller VERITASSERVER
Clustering Mode normal

Note that the system will make a note of these parameters, but it will not attempt to join the specified domain. That will happen only when the CIFS server is started the next time using the `server` command.

Starting the CIFS server after all domain-related parameters have been set.

```
CIFS> server start
```

```
The skew of the system clock with respect to Domain controller is: 3 seconds

Time on Domain controller : Fri November 30 06:00:03 2008
Time on this system : Fri November 30 06:00:00 PDT 2008

If the above clock skew is greater than that allowed by the server, then the system won't be able to join the AD domain

Enter password for user 'administrator':

Trying to become a member in AD domain VERITASDOMAIN.COM ...

Joined domain VERITASDOMAIN.COM OK
Starting CIFS Server..
```

Display the status of the CIFS server.

```
CIFS> server status
CIFS Status on test_01 : ONLINE
CIFS Status on test_02 : ONLINE

Homedefirfs : fs
Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Domain Controller : VERITASSERVER
Domain User : administrator
Clustering Mode : normal
```

Display the status of the CIFS server if allowed_trusted_domain is set to yes.

```
CIFS> server status
CIFS Status on test_01 : ONLINE
CIFS Status on test_02 : ONLINE

Homedefirfs : fs
Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Domain Controller : VERITASSERVER
```
Domain User: administrator
Clustering Mode: normal
Trusted Domains: VERITASDOMAIN1 [VERITASDOMAIN2] VERITASDOMAIN3

Note: Domain name with square bracket means this trusted domain is obsolete.

Stop the CIFS server.

cIFS> server stop
Stopping CIFS Server.....Success.

Exporting a directory fs1/dir1 in ctdb clustering mode.

ctdb.CIFS> share add fs1/dir1 share1 rw,full_acl
Exporting CIFS filesystem : share1 ..Success.

ctdb.CIFS> share show
<table>
<thead>
<tr>
<th>ShareName</th>
<th>FileSystem</th>
<th>ShareOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>share1</td>
<td>fs1/dir1</td>
<td>owner=root,group=root,fs_mode=755,rw,full_acl</td>
</tr>
</tbody>
</table>

Migration from ctdb clustering mode to normal clustering mode.

1. Check the status of the CIFS server.

ctdb.CIFS> server status
CIFS Status on ctdb_01 : ONLINE
CIFS Status on ctdb_02 : ONLINE

Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Workgroup : VERITASDOMAIN
Domain Controller : veritasdomain.veritas.com
Domain User : administrator
Clustering Mode : ctdb

2. List the shares and homedir.

ctdb.CIFS> share show
<table>
<thead>
<tr>
<th>ShareName</th>
<th>FileSystem</th>
<th>ShareOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>share1</td>
<td>fs1/Veritas Access</td>
<td>owner=root,group=root,fs_mode=755,rw,noguest</td>
</tr>
<tr>
<td>share2</td>
<td>fs1/Veritas Access</td>
<td>owner=root,group=root,fs_mode=755,ro,guest</td>
</tr>
<tr>
<td>share3</td>
<td>fs3</td>
<td>owner=root,group=root,fs_mode=1777</td>
</tr>
<tr>
<td>share4</td>
<td>fs4</td>
<td>owner=root,group=root,fs_mode=1777,rw</td>
</tr>
</tbody>
</table>

ctdb.CIFS> homedir show
<table>
<thead>
<tr>
<th>UserName</th>
<th>DomainName</th>
</tr>
</thead>
<tbody>
<tr>
<td>usr1</td>
<td>LOCAL</td>
</tr>
<tr>
<td>administrator</td>
<td>VERITASDOMAIN</td>
</tr>
</tbody>
</table>

3. Stop the CIFS server and set clustering mode to normal.

ctdb.CIFS> server stop
Disabling membership in AD domain VERITASDOMAIN.COM
Enter password for user 'administrator':
Left AD domain VERITASDOMAIN.COM

5.1. cifs
Stopping CIFS Server......Success.

ctdb.CIFS> set clustering_mode normal
Global option updated. Note: Restart the CIFS server.

4. Start the CIFS server in normal clustering mode.

ctdb.CIFS> server start
Uninstalling 'ctdb' Clustering Mode..............Success.
Installing 'normal' Clustering Mode...........Success.

The skew of the system clock with respect to Domain controller veritasdomain.veritas.com (10.209.110.210) is: 9 seconds

Time on Domain controller : Thu Aug 19 16:54:03 2010
Time on this system : Thu Aug 19 16:53:54 IST 2010

If the above clock skew is greater than that allowed by the server, then the system won't be able to join the AD domain

Trying to become a member in AD domain VERITASDOMAIN.COM ...

Enter password for user 'administrator':
Joined domain VERITASDOMAIN.COM OK
ACCESS cifs WARNING V-288-0 Migration of following shares are not supported in normal clustering mode

<table>
<thead>
<tr>
<th>Sharename</th>
<th>FS Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>share1</td>
<td>fs1/Veritas Access</td>
</tr>
<tr>
<td>share2</td>
<td>fs1/Veritas Access</td>
</tr>
</tbody>
</table>

Starting CIFS Server.....Success.

5. Check the shares and home directory after migrating to normal clustering modes.

ctdb.CIFS> share show
ShareName  FileSystem ShareOptions
share3      fs3  owner=root,group=root,fs_mode=1777
share4      fs4  owner=root,group=root,fs_mode=1777,rw

ctdb.CIFS> homedir show
UserName  DomainName
usr1      LOCAL
administrator VERITASDOMAIN

Note: You can see that directory level share cannot be migrated to normal clustering mode. Rest of the share and home directory are migrated perfectly.

Migration from normal clustering mode to ctdb clustering mode.

1. Check the server status to confirm that the current clustering mode is normal.

ctdb.CIFS> server status
CIFS Status on ctdb_01 : ONLINE
CIFS Status on ctdb_02 : ONLINE

Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
2. List the shares and the homedir.

```
ctdb.CIFS> share show
ShareName FileSystem ShareOptions
share3          fs3  owner=root,group=root,fs_mode=1777
share4          fs4  owner=root,group=root,fs_mode=1777,rw
```

```
ctdb.CIFS> homedir show
UserName       DomainName
usr1            LOCAL
administrator   VERITASDOMAIN
```

3. Now stop the CIFS server and change the clustering mode to the `ctdb` mode.

```
ctdb.CIFS> server stop
Stopping CIFS Server.....Success.
ctdb.CIFS> set clustering_mode ctdb
Global option updated. Note: Restart the CIFS server.
```

4. Start the CIFS server in `ctdb` clustering mode and check the server status.

```
ctdb.CIFS> server start
Disabling membership in AD domain VERITASDOMAIN.COM
Enter password for user 'administrator':
Left AD domain VERITASDOMAIN.COM
Uninstalling 'normal' Clustering Mode........Success.
Installing 'ctdb' Clustering Mode.........Success.
Starting CIFS Server....
The skew of the system clock with respect to Domain controller veritasdomain.veritas.com (10.209.110.210) is: 9 seconds
Time on Domain controller : Thu Aug 19 17:07:19 2010
Time on this system : Thu Aug 19 17:07:10 IST 2010
If the above clock skew is greater than that allowed by the server, then the system won't be able to join the AD domain
Trying to become a member in AD domain VERITASDOMAIN.COM ...
Enter password for user 'administrator':
Joined domain VERITASDOMAIN.COM OK
..Success.
ctdb.CIFS> server status
CIFS Status on ctdb_01 : ONLINE
CIFS Status on ctdb_02 : ONLINE
Security : ads
Domain membership status : Enabled
```

5.1. cifs
5. Verify that all shares and home directory are properly migrated to the ct db clustering mode.

```
ctdb.CIFS> share show
   ShareName  FileSystem  ShareOptions
   share1     fs1         owner=root,group=root,fs_mode=1777,rw,full_acl
   share3     fs3         owner=root,group=root,fs_mode=1777
   share4     fs4         owner=root,group=root,fs_mode=1777,rw
```

```
ctdb.CIFS> homedir show
   UserName  DomainName
   usr1      LOCAL
   administrator  VERITASDOMAIN
```

5.1.5 SEE ALSO

server(1), share(1)
5.2 homedir

5.2.1 SYNOPSIS

homedir set username [domainname] [fs_name]
homedir delete username [domainname]
homedir deleteall
homedir show [username] [domainname]

5.2.2 DESCRIPTION

The homedir commands manage the home directories for the users.

5.2.3 OPTIONS

homedir set username [domainname] [fs_name] Set the homedir for the given user. If the home directory does not exist for the given user, this command creates that user’s home directory. Use fs_name to specify the home directory file system where the user’s home directory is created. Otherwise, the user’s home directory is created on the home directory file system that has the fewest home directories. Use storage quota cifshomedir set to set the quota value for the user, otherwise the value set from the storage quota cifshomedir setdefault is used to configure the quota limit. If either user or default quota is not set, 0 is taken as the default value, which is treated as an unlimited quota.

homedir delete username [domainname] Delete the home directory of the given user.

homedir deleteall Delete all of the home directories on the homedir file system.

homedir show [username] [domainname] Display the homedir usage information.

5.2.4 EXAMPLES

Set the homedir for the given user.

CIFS> homedir set usr1 local
CIFS>

Delete the home directory of user2.

CIFS> homedir delete user2
Do you want to delete homedir for user user2 (y/n): y
Success: Home directory deleted for CIFS local user: user2

Display the home directory usage information.

CIFS> homedir show
UserName   DomainName
user1       LOCAL
user2       LOCAL
5.2.5 SEE ALSO

set(1)
5.3 local

5.3.1 SYNOPSIS

local user add username [grouplist]
local password username
local user delete username
local user show [username]
local group add groupname
local group delete groupname
local group show [groupname]
local user members username grouplist

5.3.2 DESCRIPTION

The local commands add, delete, or display CIFS user(s)/group(s).

5.3.3 OPTIONS

    grouplist  Comma-separated list of group names.

    local user add username [grouplist]  Add the local CIFS user. This user gets authenticated when security is set to user.

    local password username  Reset password for the local CIFS user.

    local user delete username  Delete the specified CIFS user.

    local user show [username]  Show UID and group(s) details of the given username.

    local group add groupname  Add the local CIFS group.

    local group delete groupname  Delete the local CIFS group.

    local group show [groupname]  Show the list of available local CIFS groups. If `groupname` is specified, it shows all the users belonging to that group.

    local user members username grouplist  Add the local CIFS user to the given groups in the grouplist.

5.3.4 EXAMPLES

Add a local CIFS group grp1.

```
CIFS> local group add grp1
Adding GROUP : grp1
Success: Group grp1 created successfully
```

Create the new CIFS user usr1 and assign it to existing groups grp1.

```
```
CIFS> local user add usr1 grpl
Input password for usr1.
Enter password:
Re-enter password:
Adding USER : usr1
Success: User usr1 created successfully

Reset password for the local CIFS user usr1.

CIFS> local password usr1
Changing password for usr1.
New password:
Re-enter new password:
Password changed for user: 'usr1'

Show the list of local CIFS users.

CIFS> local user show
List of Users
---------
usr1

Delete the local CIFS user usr1.

CIFS> local user delete usr1
Deleting User: usr1
Success: User usr1 deleted successfully

5.3.5 SEE ALSO

server(1)
5.4 mapuser

5.4.1 SYNOPSIS

mapuser add CIFSusername domainname NFSusername
mapuser remove CIFSusername [domainname]
mapuser show [CIFSusername] [domainname]

5.4.2 DESCRIPTION

The mapuser commands add, remove, or display the mapping between CIFS and NFS users. Typically a CIFSusername is a user coming from the AD server (domainname), or a locally created CIFS user on this system (local). A NFSusername is a user coming from a locally created CIFS user on this system or from a NIS/LDAP server configured in the network section. To make sure user mappings work properly with a NIS/LDAP server, the nsswitch setting may need to be adjusted in the network section.

5.4.3 OPTIONS

mapuser add CIFSusername domainname NFSusername Map CIFS user to NFS user. This mapping is useful when the same file system is accessed using both CIFS and NFS. This functionality can also be used to map multiple users to a single username to share common data. Note: If *** is specified both for the CIFS user and the NFS user, mappings are created automatically between the same name user between CIFS and NFS users on the CIFS server when such user logs on.

mapuser remove CIFSusername [domainname] Remove the mapping between CIFS and NFS user. It may be possible that the CIFS user may not be able to access its previous data after removing the mapping. Default domain is local. Note: If *** is specified, no more mappings are created between the same name CIFS and NFS users, however the already created same name mappings are left in the user mapping list on the CIFS server.

mapuser show [CIFSusername] [domainname] Show the mapping between the CIFS and the NFS user. If the CIFS username is not specified, it shows all the existing mappings. Default domain name is local.

5.4.4 EXAMPLES

Map CIFS user to NFS user.

CIFS> mapuser add administrator VERITASDOMAIN.COM nfsusr1

Add mappings between all the same name CIFS and NFS users.

CIFS> mapuser add * VERITASDOMAIN.COM *

Remove the mapping between the CIFS and the NFS user.

CIFS> mapuser remove administrator VERITASDOMAIN.COM

Remove the mappings between the same name CIFS and NFS users.
CIFS> mapuser remove * VERITASDOMAIN.COM

Show the mappings between the CIFS and the NFS user.

<table>
<thead>
<tr>
<th>CIFSUserName</th>
<th>DomainName</th>
<th>NFSUserName</th>
</tr>
</thead>
<tbody>
<tr>
<td>administrator</td>
<td>VERITASDOMAIN</td>
<td>nfsusr1</td>
</tr>
</tbody>
</table>

5.4.5 SEE ALSO

share(1)
5.5 server

5.5.1 SYNOPSIS

server [start|stop|status]

5.5.2 DESCRIPTION

Start, stop, or display the status of the CIFS resources. All variable settings made using the set command come into effect only when the server is restarted. For example, set can be used to set the security to ads or to a value other than ads, but the server joins or leaves the active directory domain only when the server is restarted after issuing the set command. One exception is the case when the server is already stopped, and later security is set to a value other than ads.

5.5.3 OPTIONS

server [start|stop|status] Start, stop, or check the status of the CIFS resources.

5.5.4 EXAMPLES

Starting the CIFS server after all domain-related parameters have been set.

```
CIFS> server start
The skew of the system clock with respect to Domain controller is: 3 seconds
Time on Domain controller : Fri November 30 06:00:03 2008
Time on this system : Fri November 30 06:00:00 PDT 2008
If the above clock skew is greater than that allowed by the server, then the system won't be able to join the AD domain
Enter password for user 'administrator':
Trying to become a member in AD domain VERITASDOMAIN.COM ...
Joined domain VERITASDOMAIN.COM OK
Starting CIFS Server..
```

Display the status of CIFS server.

```
CIFS> server status
CIFS Status on test_01 : ONLINE
CIFS Status on test_02 : ONLINE
Homedirfs : fs
Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Domain Controller : VERITASSERVER
Domain User : administrator
Clustering Mode : normal
```

Display the status of the CIFS server if allowed_trusted_domain is set to yes.
CIFS> server status
CIFS Status on test_01 : ONLINE
CIFS Status on test_02 : ONLINE

Homedirfs : fs
Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Domain Controller : VERITASSERVER
Domain User : administrator
Clustering Mode : normal
Trusted Domains : VERITASDOMAIN1 [VERITASDOMAIN2] VERITASDOMAIN3

Note: Domain name with square brackets means this trusted domain is obsolete.

Stop the CIFS server.

CIFS> server stop
Stopping CIFS Server.....Success.

5.5.5 SEE ALSO

set(1), share(1)
5.6 set

5.6.1 SYNOPSIS

set domaincontroller servernames
set domainuser username
set domain domainname
set workgroup workgroup
set allow_trusted_domains yes|no [trusted_domains]
set ntlm_auth yes|no
set security ads|user
set idmap_backend ldap [idmap_ou] [uid_range]
set idmap_backend rid [uid_range]
set idmap_backend hash
set idmap_backend ad [uid_range]
set homedirfs [filesystemlist] [full_acl]
set aio_size size
set data_migration yes|no
set clustering_mode normal|ctdb

5.6.2 DESCRIPTION

The set commands allow the user to set various parameters required for CIFS functioning.

5.6.3 OPTIONS

set domaincontroller servernames Set the comma-separated list of domain controller server names. A domain controller can either be an active directory server or a Windows NT 4.0 domain controller.

set domainuser username Set the name of the domain user. This username is used for authentication for the domain join operation.

set domain domainname Set the domain name. This also sets the WORKGROUP of the system.

set workgroup workgroup Set the workgroup name. If name of the WORKGROUP or NetBIOS domain name is different from the domain name, use this command to set workgroup name.

set allow_trusted_domains yes|no [trusted_domains] If allow_trusted_domains is set to yes, then multiple domain environments are allowed. If set to no, multiple domain environments are not allowed. Note: This option cannot be set to yes if security mode is user.

The user can also specify the trusted domains that allow access to the CIFS server when this option is set to yes and the idmap backend is set to rid or ad. By default all the trusted domains are included in the configuration.

Default allow_trusted_domains Value: no
set ntlm_auth yes|no  If ntlm_auth is set to no, then an NTLMv2 response needs to be sent by the client. If set to yes, it attempts to authenticate users using the NTLM-encrypted password response.

Default ntlm_auth Value: yes

set security ads|user  Set CIFS security to user (user-level security that a client must log on with a valid username and password) or ads (CIFS server acts as a domain member in an active directory). Before setting the security to ads, it is required to set domain, domaincontroller, and domainuser. When the user executes the server start command, the CIFS server asks for the password corresponding to the domainuser to join in the AD. If using security as ads, make sure that the clock of the AD server and the CIFS server is set to the same time. Use the NTP server if possible. If using security as ads, make sure that the clock of the AD server and Veritas Access is set to the same time. Use the NTP server if possible.

Default security Value: user

set idmap_backend ldap [idmap_ou] [uid_range]  This option tells the CIFS server to obtain SID to UID/GID mappings from a common LDAP backend. The LDAP server used for this has to be configured through the LDAP sub-section in the network section. Trusted domains are allowed if allow_trusted_domains is set to yes. The idmap_ou is optional and set to cifsidmap. By default, the user can specify it if the CIFS idmap OrganizationalUnitName(OU) is named differently on the LDAP server. The uid_range is optional and set to 10000-1000000 by default.

set idmap_backend rid [uid_range]  The user can use this option to get the unique SID to UID/GID mappings based on RID and LOW_RANGE_ID. Trusted domains are allowed if allow_trusted_domains is set to yes.

The uid_range is set to 10000-1000000 by default, change it in cases where there are more than 1,000,000 users existing on the local Veritas Access cluster, joined active directory, or trusted domains. Note: Do not attempt to modify LOW_RANGE_ID (10000) if there is user data on the CIFS server, it may lead to data access denied for the UID changes.

set idmap_backend hash  User can use this option to get the unique SID to UID/GID mappings by the implemented hashing algorithm. Trusted domains are allowed if allow_trusted_domains is set to yes.

set idmap_backend ad [uid_range]  User can use this option to get the unique UID/GID from domain by reading id mappings from an AD server that uses RFC2307/SFU schema extensions, this is a readonly idmap backend. Trusted domains are allowed if allow_trusted_domains is set to yes. A valid user from a domain or a trusted domain should have a UID as well as a GID for the user's primary group.

The uid_range is set to 10000-1000000 by default, change it in cases where there are more than 1,000,000 users existing on the local Veritas Access cluster, joined active directory, or trusted domains. Note: ID range is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

set homedirfs [filesystemlist] [full_acl]  Set the given list of file systems to be used for the home directory. All of the home directories of the users are created in these file systems. filesystem is a comma-separated list of file system names. full_acl can be set as an option. Automatic migration of the content of users (that is, users’ home directories) from one file system to another file system while switching homedir is not supported. So if an administrator changes homedir from fs1 to fs2, then the home directories of the user do not migrate from fs1 to fs2 automatically.

set aio_size size  Set aio_fork option. If size is not 0, then enable aio_fork and set it as aio read/write size. If it is 0, then disable aio_fork and set 0 to aio read/write size.

set data_migration yes|no  The user can use this option to enable data migration from a Windows machine by a domain administrator, when ACL information for files or directories should be preserved. The ROBOCOPY command from the Windows Resource Kit Tools is required to complete
this task. Set the option to yes and restart the CIFS server, and then the data migration mode is enabled. Set the option to no after data migration completes for CIFS server security.

**set clustering mode normal|ctdb** Set the clustering mode for the CIFS server. There are two clustering modes available with Veritas Access, normal and ctdb. Each clustering mode supports all of the three operating modes. The CTDB clustering mode is a different clustered implementation of Veritas Access CIFS, which supports all the features that are supported by normal clustering mode as well as some additional features. Additional features supported in CTDB clustering mode: Directory-level share support, Multi-instance share export of a file system/directory, and better load balancing. Veritas Access supports automated and seamless migration of shares and homedirectories from one mode to another. However while migrating from CTDB to normal clustering mode, some of the shares get discarded that are not supported in normal clustering mode.

### 5.6.4 EXAMPLES

Setting the domain parameters for joining an active directory or NT domain. In this example, the name of the domain is set to VERITASDOMAIN.COM, domain user is set to administrator, and domain controller for the domain VERITASDOMAIN.COM is set to VERITASSERVER.

```
CIFS> set domain `\"VERITASDOMAIN.COM\"`
Global option updated. Note: Restart the CIFS server.
CIFS> set domainuser `\"administrator\"`
Global option updated. Note: Restart the CIFS server.
CIFS> set domaincontroller `\"VERITASSERVER\"`
Global option updated. Note: Restart the CIFS server.
```

After setting all the above domain parameters, you can set the security to either ads if the domain controller is an active directory server, or you can set the security to domain if the domain controller is an NT domain controller.

```
CIFS> set security `\"ads\"`
Global option updated. Note: Restart the CIFS server.
```

Note that the system will make a note of these parameters, but it will not attempt to join the specified domain. That happens only when the CIFS server is started the next time using the server command.

### 5.6.5 SEE ALSO

server(1), share(1)
5.7 share

5.7.1 SYNOPSIS

share add filesystem sharename [@virtual_ip] [cifsoptions]
share modify sharename [@virtual_ip] [cifsoptions]
share delete sharename [@virtual_ip]
share show [sharename]
share allow sharename @group1 [..., @group2, user1, user2, ...]
share deny sharename @group1 [..., @group2, user1, user2, ...]

5.7.2 DESCRIPTION

The share commands add, delete, or display CIFS shares.

5.7.3 OPTIONS

  cifsoptions Comma-separated list of export options for a CIFS share: {ro, rw, guest, noguest, oplocks, nooplocks, full_acl, no_full_acl, enable_encryption, disable_encryption, shadow_copy, hide_unreadable, veto_sys_files, enable_durable_handles, owner=ownername, group=groupname, fs_mode=fspermission, dir_mask=dirpermission, create_mask=filepermission, allow=user+@group, deny=user+@group, max_connections=connections}. The default export options are{ro, noguest, oplocks, no_full_acl, fs_mode=1777, dir_mask=775, create_mask=775, allow=all}.

share add filesystem sharename [@virtual_ip] [cifsoptions] Export the file system with the given sharename. The new options are updated after the command is run. In both clustering modes, you can give the directory path instead of the file system. While specifying the directory path, make sure it always starts with the file system name (Note: not with the mount point /vx). If @virtual_ip is specified, the share can only be accessed by virtual_ip.

share modify sharename [@virtual_ip] [cifsoptions] Re-export the file system with the given sharename. The new options are updated after the command is run. In both clustering modes, you can give the directory path instead of the file system. While specifying the directory path, make sure it always starts with file system name (Note: not with the mount point /vx). If @virtual_ip is specified, the share can only be accessed by virtual_ip.

share delete sharename Unexport the share with the name sharename.

share show [sharename] List all the exported resources. If sharename is specified, then it prints all the details of the given sharename.

share allow sharename @group1 [..., @group2, user1, user2, ...] Allow only the specified users and groups to access the share. If all is specified, then default access restrictions are restored on the share. User or group separator can be a comma or a plus symbol, double backslash should be added between the domain name and the user or group in cases where the allowed one comes from the trusted domain.

share deny sharename @group1 [..., @group2, user1, user2, ...] Deny the specified users and groups to access the share. If all is specified, then all the users and groups are not able to access the share. User or group separator can be a comma or a plus symbol, double backslash should be added between the domain name and the user or group in cases where the denied one comes from the trusted domain.
5.7.4 EXAMPLES

Export the file system fs1 with name share1.

```
CIFS> share add fs1 share1
Exporting CIFS filesystem : share1 ...
```

Display the list of shares exported over CIFS.

```
CIFS> share show
ShareName  FileSystem  ShareOptions
share1     fs1         owner=root,group=root
```

Unexport the share with the name share1.

```
CIFS> share delete share1
Unexporting CIFS share : share1 ....
```

Allow user user1 and group group1 to access the share share1.

```
CIFS> share allow share1 user1,@group1
Warning: Modifying an already existing share.
........Done
```

Allow trusted domain user user1 and group group1 to access the share share1.

```
CIFS> share allow share1 domain\\user1,@domain\\group1
Warning: Modifying an already existing share.
........Done
```

Deny user user1 and group group1 to access the share share1.

```
CIFS> share deny share1 user1,@group1
Warning: Modifying an already existing share.
........Done
```

Deny trusted domain user user1 and group group1 to access the share share1.

```
CIFS> share deny share1 domain\\\\user1,@domain\\\\group1
Warning: Modifying an already existing share.
........Done
```

Exporting a directory as a CIFS share, you should switch to the ctdb clustering mode.

1. Check the status of the CIFS server to confirm that the current clustering mode is ctdb.

```
ctdb.CIFS> server status
CIFS Status on ctdb_01 : ONLINE
CIFS Status on ctdb_02 : ONLINE

Security : ads
Domain membership status : Enabled
Domain : VERITASDOMAIN.COM
Workgroup : VERITASDOMAIN
Domain Controller : veritasdomain.veritas.com
Domain User : administrator
Clustering Mode : ctdb
```

2. Export a directory as a CIFS share.
ctdb.CIFS> share add fs1/dir1 share1 rw,full_acl
Exporting CIFS filesystem : share1 ..Success.

3. List the shares.

<table>
<thead>
<tr>
<th>ShareName</th>
<th>FileSystem</th>
<th>ShareOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>share1</td>
<td>fs1/dir1</td>
<td>owner=root,group=root,fs_mode=755,rw,full_acl</td>
</tr>
</tbody>
</table>

ctdb.CIFS> share show

4. If a directory name contains a space, then it should be entered using double quotes (".

<table>
<thead>
<tr>
<th>ShareName</th>
<th>FileSystem</th>
<th>ShareOptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>share2</td>
<td>fs1/dir2 a</td>
<td>owner=root,group=root,fs_mode=755,rw</td>
</tr>
<tr>
<td>share1</td>
<td>fs1/dir1</td>
<td>owner=root,group=root,fs_mode=755,rw,full_acl</td>
</tr>
</tbody>
</table>

ctdb.CIFS> share show

5. Modifying an existing share.

ctdb.CIFS> share modify share2 ro,full_acl
Warning: Modifying an already existing share.
...Done

ctdb.CIFS> share show

5.7.5 SEE ALSO

server(1)
5.8 show

5.8.1 SYNOPSIS

show

5.8.2 DESCRIPTION

The show command displays the list of global options and their values. These are the settings that have been configured primarily with the set command.

5.8.3 EXAMPLES

Display the list of global options.

```
CIFS> show

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>netbios name</td>
<td>test</td>
</tr>
<tr>
<td>ntlm auth</td>
<td>yes</td>
</tr>
<tr>
<td>allow trusted domains</td>
<td>no</td>
</tr>
<tr>
<td>homedirfs</td>
<td></td>
</tr>
<tr>
<td>aio size</td>
<td>0</td>
</tr>
<tr>
<td>idmap backend</td>
<td>rid:10000-1000000</td>
</tr>
<tr>
<td>workgroup</td>
<td>VERITASDOMAIN</td>
</tr>
<tr>
<td>security</td>
<td>ads</td>
</tr>
<tr>
<td>Domain</td>
<td>VERITASDOMAIN.COM</td>
</tr>
<tr>
<td>Domain user</td>
<td>administrator</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>VERITASSERVER</td>
</tr>
<tr>
<td>Clustering Mode</td>
<td>normal</td>
</tr>
</tbody>
</table>
```

5.8.4 SEE ALSO

set(1)
6.1 cluster

6.1.1 SYNOPSIS

reboot nodename
show[currentload]
shutdown nodename
add ipaddr1 [, ipaddr2,...]
del nodename1 [, nodename2,...]

6.1.2 DESCRIPTION

The cluster commands allow you to view the nodes in the cluster and their states. You can add, remove, reboot, or shutdown nodes in the cluster configuration.

6.1.3 OPTIONS

**nodename** The node on which the operation takes place. A value of all indicates the operation takes place on all of the nodes in the cluster. The value all does not apply to the del command.

**ipaddr** The accessible IP address of the node to be added to the cluster.

**reboot nodename** Reboot a node or all of the nodes in the cluster. To reboot a node, specify the nodename as it is displayed in the cluster show command. To reboot all the nodes in the cluster use all for nodename.

**show** Display the nodes in the cluster, their states, CPU load, and network load, during the past 15 minutes. It also displays information about nodes that are being added to the cluster, deleted from the cluster and nodes on which upgrade is in progress.

**show [currentload]** If you specify currentload, the load statistics show the CPU load, and network load for the 5 seconds after the command is issued.
**shutdown nodename** Shut down a node or all of the nodes in the cluster. To shut down a node, specify the *nodename* as it is displayed in the `cluster show` command. To shut down all the nodes in the cluster, use `all` for *nodename*.

**add ipaddr1 [, ipaddr2,...]** Add one or more nodes into the cluster. The *ipaddr* should be known before the `add` operation. The cluster must be running and the new nodes must have the required OS installed.

**del nodename1 [, nodename2,...]** Delete one or more nodes from the cluster. The specified nodes must be in the cluster but can not be the console node. You cannot delete all of the running nodes in the cluster. After a node is successfully deleted, the node is still accessible at the IP address until the node is rebooted. After the reboot, the node frees the used IP resources and is assigned to the original ip.

### 6.1.4 EXAMPLES

Display the current state of all the nodes in the cluster and their loads, during the past 15 minutes.

```yaml
Cluster> show
Node | State | CPU(15 min) | pubeth0(15 min) | pubeth1(15 min) |
---- | ----- | ----------- | ---------------- | ----------------|
---- | ----- | ----------- | ---------------- | ----------------|
test_1 | RUNNING | 1.35 | 0.00 | 0.00 |
test_2 | RUNNING | 1.96 | 0.00 | 0.00 |
test_3 | FAULTED |       |       |       |
```

**Nodes in Transition**

<table>
<thead>
<tr>
<th>Node/IP</th>
<th>Operation</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.58.202</td>
<td>Add node</td>
<td>FAILED</td>
<td>Installing packages</td>
</tr>
<tr>
<td>test_6</td>
<td>Delete node</td>
<td>ONGOING</td>
<td>Removing node</td>
</tr>
<tr>
<td>test_4,test_5</td>
<td>Rolling upgrade</td>
<td>ONGOING</td>
<td>Rolling upgrade phase 2</td>
</tr>
</tbody>
</table>

Display the CPU and network loads collected for the next 5 seconds.

```yaml
Cluster> show currentload
Node | State | CPU(5 sec) | pubeth0(5 sec) | pubeth1(5 sec) |
---- | ----- | ----------- | ---------------- | ----------------|
---- | ----- | ----------- | ---------------- | ----------------|
test_1 | RUNNING | 1.35 | 0.00 | 0.00 |
test_2 | RUNNING | 1.96 | 0.00 | 0.00 |
test_3 | FAULTED |       |       |       |
```

Shut down a node in the cluster.

```yaml
Cluster> shutdown test_4
Stopping Cluster processes on test_4
Sent shutdown command to test_4. SSH sessions to test_4 may terminate.
```

Shut down all nodes in the cluster.

```yaml
Cluster> shutdown all
Stopping Cluster processes on all
SSH sessions to all nodes may terminate.
Sent shutdown command to test_2
Sent shutdown command to test_3
Sent shutdown command to test_4
Sent shutdown command to test_1
```
Reboot a node in the cluster.

```
Cluster> reboot test_4
Stopping Cluster processes on test_4
Sent reboot command to test_4. SSH sessions to test_4 may terminate.
```

Reboot all nodes in the cluster.

```
Cluster> reboot all
Stopping Cluster processes on all
SSH sessions to all nodes may terminate.
Sent reboot command to test_2
Sent reboot command to test_3
Sent reboot command to test_4
Sent reboot command to test_1
```

6.1.5 SEE ALSO

add(1), del(1), reboot(1), show(1), shutdown(1)
6.2 add

6.2.1 SYNOPSIS

\texttt{add ipaddr1 [, ipaddr2,...]}

6.2.2 DESCRIPTION

The cluster \texttt{add} command adds one or more nodes into the running cluster. Provide the IP address of each new node. To specify multiple nodes, separate the IP addresses with commas. The cluster needs to be running and the new nodes must have the required OS installed.

6.2.3 EXAMPLES

Add a node 10.10.10.10 into the cluster.

\begin{verbatim}
Cluster> add 10.10.10.10
\end{verbatim}

Add 2 nodes 10.10.10.10,10.10.10.11 into the cluster.

\begin{verbatim}
Cluster> add 10.10.10.10,10.10.10.11
\end{verbatim}

6.2.4 SEE ALSO

del(1), reboot(1), show(1), shutdown(1)
6.3 del

6.3.1 SYNOPSIS

del nodename1 [, nodename2,...]

6.3.2 DESCRIPTION

The cluster `del` command deletes one or more nodes from current cluster. The specified nodes must be in the cluster but cannot be the console node. You cannot delete all the running nodes in the cluster.

After a node is successfully deleted, the node is still accessible at the IP address until the node is rebooted. After the reboot, the node frees the used IP resources and is assigned to the original IP.

6.3.3 EXAMPLES

Delete a node test_02 from the cluster.

```
Cluster> del test_02
```

Delete 2 nodes test_02,test_03 from the cluster.

```
Cluster> del test_02,test_03
```

6.3.4 SEE ALSO

add(1), reboot(1), show(1), shutdown(1)
6.4 reboot

6.4.1 SYNOPSIS

reboot nodename

6.4.2 DESCRIPTION

The cluster reboot command reboots a node or all of the nodes in the cluster. To reboot a node in the cluster, specify the nodename as it is displayed in the cluster show command. To reboot all of the nodes in the cluster, use all for nodename.

6.4.3 OPTIONS

- **nodename** Node on which the operation takes place. A value of all indicates the operation takes place on all nodes of the cluster.
- **reboot nodename** Reboots a node or all of the nodes in the cluster. To reboot a node in the cluster, specify the nodename as it is displayed in the cluster show command. To reboot all of the nodes in the cluster, use all for nodename.

6.4.4 EXAMPLES

Reboots a node in the cluster.

```
Cluster> reboot test_4
Stopping Cluster processes on test_4
Sent reboot command to test_4. SSH sessions to test_4 may terminate.
```

Reboots all of the nodes in the cluster.

```
Cluster> reboot all
Stopping Cluster processes on all
SSH sessions to all nodes may terminate.
Sent reboot command to test_2
Sent reboot command to test_3
Sent reboot command to test_4
Sent reboot command to test_1
```

6.4.5 SEE ALSO

show(1), shutdown(1)
6.5 show

6.5.1 SYNOPSIS

show [currentload]

6.5.2 DESCRIPTION

The cluster show command displays the nodes in the cluster, their states, CPU load, and network load during the past 15 minutes. It also displays information about nodes that are being added to the cluster, deleted from the cluster and nodes on which upgrade is in progress. The rx and tx columns display statistics of received and transmitted bytes respectively.

6.5.3 OPTIONS

 show [currentload] If you specify currentload, the load statistics show the CPU load, and network load for the 5 seconds after the command is issued.

6.5.4 EXAMPLES

Display the current state of all of the nodes in the cluster and their loads during the past 15 minutes.

Cluster> show

Node State CPU(15 min) pubeth0(15 min) pubeth1(15 min)
---- ----- ----------- -------- -------- -------- --------
test_1 RUNNING 1.35 0.00 0.00 0.00 0.00
test_2 RUNNING 1.96 0.00 0.00 0.00 0.00
test_3 FAULTED

Nodes in Transition

<table>
<thead>
<tr>
<th>Node/IP</th>
<th>Operation</th>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.200.58.202</td>
<td>Add node</td>
<td>FAILED</td>
<td>Installing packages</td>
</tr>
<tr>
<td>test_6</td>
<td>Delete node</td>
<td>ONGOING</td>
<td>Removing node</td>
</tr>
<tr>
<td>test_4,test_5</td>
<td>Rolling upgrade</td>
<td>ONGOING</td>
<td>Rolling upgrade phase 2</td>
</tr>
</tbody>
</table>

Show the CPU and network loads collected for the next 5 seconds.

Cluster> show currentload

Node State CPU(5 sec) pubeth0(5 sec) pubeth1(5 sec)
---- ----- ----------- -------- -------- -------- --------
test_1 RUNNING 1.35 0.00 0.00 0.00 0.00
test_2 RUNNING 1.96 0.00 0.00 0.00 0.00
test_3 FAULTED

6.5.5 SEE ALSO

reboot(1), shutdown(1)
6.6 shutdown

6.6.1 SYNOPSIS

shutdown nodename

6.6.2 DESCRIPTION

The cluster shutdown command shuts down the nodes in the cluster.

6.6.3 OPTIONS

nodename  Node on which the operation takes place. A value of all indicates the operation takes place on all of the nodes in the cluster.

shutdown nodename  Shut down a node or all of the nodes in the cluster. To shut down a node in the cluster, specify the nodename, as it appears in the cluster show command. To shut down all of the nodes in the cluster, use all for nodename.

6.6.4 EXAMPLES

Shut down a node in the cluster.

Cluster> shutdown test_4
Stopping Cluster processes on test_4
Sent shutdown command to test_4. SSH sessions to test_4 may terminate.

Shut down all of the nodes in the cluster.

Cluster> shutdown all
Stopping Cluster processes on all
SSH sessions to all nodes may terminate.
Sent shutdown command to test_2
Sent shutdown command to test_3
Sent shutdown command to test_4
Sent shutdown command to test_1

6.6.5 SEE ALSO

reboot(1), show(1)
7.1 database

7.1.1 SYNOPSIS

fs create obj-type db-name fs-name size
fs destroy db-name fs-name
fs list
pool create obj-type disk1 [, disk2, ...]
pool destroy obj-type
pool list
share add obj-type export-dir [client]
share delete export-dir [client]
share show

7.1.2 DESCRIPTION

These database commands are used to create and manage storage for Oracle database clients. The storage is accessed by Oracle hosts using the Oracle Direct NFS protocol. Oracle Direct NFS (DNFS) is an optimized NFS (Network File System) client that provides faster access to NFS storage located on NAS appliances. The Oracle Database Direct NFS client integrates the NFS client functionality directly in the Oracle database. Through this integration, the I/O path between Oracle and the NFS server is optimized, providing significantly better performance. The Oracle Direct NFS client outperforms traditional NFS clients, and is simple to configure, and it provides a standard NFS client implementation across all hardware and operating system platforms.

It is recommended to group the storage according to the database objects stored in the file system. Oracle database objects are broadly divided into REDO transaction logs, archived logs, table data, index, and tempfiles. The following values for “obj-type” are available: 
- txnlog: Stores REDO transaction logs data
- archivelog: Stores archive logs
- data: Stores TABLE data of datafiles
- index: Stores INDEX data
- temp: Stores TEMPORARY files
- archivelog: Stores archive logs
7.1.3 OPTIONS

`fs create obj-type db-name fs-name size` Create a file system for database with name `db-name` to store objects of type `obj-type`. The name of the file system is `fs-name` and the size of the file system is `size`.

`fs destroy db-name fs-name` Destroy the file system with name `fs-name`.

`fs list` List file systems created for storing database files.

`pool create obj-type disk1 [, disk2,...]` Create a pool to store database objects of type `obj-type`. The `obj-type` must be one of txnlog, archivelog, data, index, or temp.

`pool destroy obj-type` Destroy the pool specified by the database `obj-type`.

`pool list` List all the pools configured for the database. `share add obj-type export-dir [client]` Share and export the file system `export-dir`. After this command, database clients are able to mount using NFS this file system on their host.

`share delete export-dir [client]` Delete (or unshare) the exported file system.

`share show` Display all the shared database file systems.

7.1.4 EXAMPLES

Here is an example of the commands to create storage for an Oracle TPCC database.

1. First create storage pools for the TPCC database.

   
   `database> pool create data vmdk0_1,vmdk0_2 database> pool create txnlog vmdk0_3 database> pool create archivelog vmdk0_4 database> pool create index vmdk0_5,vmdk0_6`

2. Next create the respective file systems.

   
   `database> fs create data tpcc data1 300g database> fs create txnlog tpcc redo1 12g database> fs create index tpcc indx1 48g database> fs create index tpcc arch1 100g`

3. Next share and export the file systems.

   
   `database> share add txnlog /vx/tpcc_redo1 database> share add data /vx/tpcc_data1 database> share add index /vx/tpcc_indx1 database> share add archivelog /vx/tpcc_arch1`

7.1.5 SEE ALSO

pool(1), fs(1), share(1)
7.2 fs

7.2.1 SYNOPSIS

fs create obj-type db-name fs-name size
fs destroy db-name fs-name
fs list

7.2.2 DESCRIPTION

These database commands are used to create and manage file systems for Oracle database clients. These file systems are accessed by Oracle hosts using the Oracle Direct NFS (DNFS) protocol. Oracle Direct NFS (DNFS) is an optimized NFS (Network File System) client that provides faster access to NFS storage located on NAS appliances.

It is recommended to group the file systems according to the database objects stored in the file systems. Oracle database objects are broadly divided into REDO transaction logs, archived logs, table data, index, and tempfiles. The following values for obj-type are available:

- txlog: Stores REDO transaction logs
- data: Stores TABLE data of datafiles
- index: Stores INDEX data
- temp: Stores TEMPORARY files
- archivelog: Stores archive logs

7.2.3 OPTIONS

fs create obj-type db-name fs-name size  Create a file system for database with name db-name to store objects of type obj-type. The name of the file system is fs-name and the size of the file system is size.

fs destroy db-name fs-name  Destroy the file system with name fs-name.

fs list List file systems created for storing database files.

7.2.4 EXAMPLES

Here is an example of the commands to create storage for an Oracle TPCC database.

1. Create file systems for the TPCC database. The following examples create four separate file systems to store respective database objects:

   database> fs create data tpcc data1 300g
   database> fs create txnlog tpcc redo1 12g
   database> fs create index tpcc indx1 48g
   database> fs create index tpcc arch1 100g

2. Display database file systems:

   database> fs list
7.2.5  SEE ALSO

pool(1), fs(1), share(1)
7.3 pool

7.3.1 SYNOPSIS

pool create obj-type disk1 [, disk2,...]
pool destroy obj-type
pool list

7.3.2 DESCRIPTION

These database pool commands are used to create and manage storage pools for an Oracle database. It is recommended to group the storage according to the database objects stored in the file system. Oracle database objects are broadly divided into REDO transaction logs, archived logs, table data, index, and tempfiles. The following values for obj-type are available.

txilog: Stores REDO transaction logs
data: Stores TABLE data of datafiles
index: Stores INDEX data
temp: Stores TEMPORARY files
archivelog: Stores archive logs

7.3.3 OPTIONS

    pool create obj-type disk1 [, disk2,...] Create a pool to store database objects of type obj-type. The
    obj-type must be one of txilog, archivelog, data, index, or temp.

    pool destroy obj-type Destroy the pool specified by the database obj-type.

    pool list List all the pools configured for the database.

7.3.4 EXAMPLES

Create storage pools for the Oracle database.

1. First create storage pools for the Oracle database.

   database> pool create data vmdk0_1, vmdk0_2
   database> pool create txilog vmdk0_3
   database> pool create archivelog vmdk0_4
   database> pool create index vmdk0_5, vmdk0_6

2. database> pool list

<table>
<thead>
<tr>
<th>POOL NAME</th>
<th>DISKS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ora_DATA_pool</td>
<td>vmdk0_1, vmdk0_2</td>
</tr>
<tr>
<td>ora_TXNLOG_pool</td>
<td>vmdk0_3</td>
</tr>
<tr>
<td>ora_ARCHIVE_pool</td>
<td>vmdk0_4</td>
</tr>
<tr>
<td>ora_INDEX_pool</td>
<td>vmdk0_5, vmdk0_6</td>
</tr>
</tbody>
</table>
7.3.5 SEE ALSO

pool(1), fs(1), share(1)
7.4 share

7.4.1 SYNOPSIS

share add obj-type export-dir [client]
share delete export-dir [client]
share show

7.4.2 DESCRIPTION

These database commands are used to export file systems created for databases using NFS. The Oracle Database Direct NFS client integrates the NFS client functionality directly in the Oracle database. Through this integration, the I/O path between Oracle and the NFS server is optimized, providing significantly better performance. The Oracle Direct NFS client outperforms traditional NFS clients, and is simple to configure, and it provides a standard NFS client implementation across all hardware and operating system platforms.

7.4.3 OPTIONS

    share add obj-type export-dir [client] Share and export the file system export-dir. After this command, database clients are able to mount using NFS this file system on their host.
    share delete export-dir [client] Delete (or unshare) the exported file system.
    share show Display all the shared database file systems.

7.4.4 EXAMPLES

Here is an example of commands to export file systems for an Oracle TPCC database.

1. Share and export the file systems for the TPCC database.

   database> share add txnlog /vx/tpcc_redol
   database> share add data /vx/tpcc_datal
   database> share add index /vx/tpcc_indxl
   database> share add archivelog /vx/tpcc_archl

2. Show the exported file systems for the database.

   database> share show

7.4.5 SEE ALSO

pool(1), fs(1), share(1)
8.1 FTP

8.1.1 SYNOPSIS

server
start|stop|status
set listen_port port_number
set listen_ipv6 yes|no
set max_connections connections_number
set max_conn_per_client connections_number
set passive_port_range port_range
set idle_timeout time_in_minutes
set allow_non_ssl yes|no
set umask file_umask
set anonymous_logon yes|no
set anonymous_login_dir login_directory
set anonymous_write yes|no
set user_logon yes|no
set homedir_path home_directory_path
set allow_delete yes|no
set security nis|ldap|ads|local
set chroot_users yes|no
set create_homedirs yes|no
show
session show
session showdetail [filter_options]
session terminate session_id
logupload url [nodename]
local user add username
local user passwd username
local user delete username
local user show
local user set bandwidth username bandwidth
local user set max_connections username number
local user set homedir username homedir

8.1.2 DESCRIPTION

The FTP commands are used to configure the FTP server. The FTP server allows files to be accessed using the File Transfer Protocol (FTP).

By default, the FTP server is not running. To start the FTP server, enter the server start command.

By default, anonymous FTP access is disabled. To enable anonymous FTP access, use set anonymous_logon yes. The UID of anonymous user is 40, GID is 49, and username is ‘ftp’. To change the default login directory of anonymous users, use set anonymous_login_dir. By default, anonymous users do not have write access to their login directory. To allow anonymous users write access to their login directories, use set anonymous_write yes.

By default, the FTP server allows plain text and SSL (secure) user logins. To allow only SSL (secure) and to reject plain text user logins, use set allow_non_ssl no.

If the create_homedirs option is set to yes, Veritas Access creates a user’s home directory on the FTP server with the same name that was retrieved from the authentication server. This directory is used internally. If the create_homedirs option is set to no, the Veritas Access administrator must manually create a directory that matches the home directory on the authentication server. Regardless of the setting of the create_homedirs option, the Veritas Access administrator must manually create the user’s directory where the user logs in. This directory is in the location specified by the homedir_path option. The directory must have execute permissions set. The following examples show the functionality for different types of users, if the homedir_path is set to /vx/fs1/ftphomes and create_homedirs option is set to yes.

For NIS users: Create the directory with username in the homedir_path. For example: /vx/fs1/ftphomes/nisuser1.

For LDAP users: Create the directory with ldapusername in the homedir_path. For example: /vx/fs1/ftphomes/ldapuser1.

For AD users: The home directory on the AD server is specified as domainname\username. The full string (domainname\username) identifies the AD user. Create the directory domainname\username in the homedir_path. For example: /vx/fs1/ftphomes/mydomain\aduser1.

For local users: If the homedir_path is set to /vx/fs1/ftphomes, Veritas Access creates the directory /vx/fs1/ftphomes/username.

If create_homedirs is set to no and user’s home directory does not exist or has not been created manually, then the login fails. If user’s home directory has been manually created, then the administrator has to ensure that the permissions have been set correctly.

If chroot_users is set to yes, then users are restricted to their home directories. If homedir_path is set to /vx/fs1/ftphomes, chroot_users is set to yes, and an AD user DOMAIN\aduser1 logs in using FTP, then the user
is restricted to /vx/fs1/ftphomes/home/DOMAIN/adsuser1. If chroot_users is set to no for the above case, then the user is restricted to /vx/fs1/ftphomes.

For security local, the chroot_users value should be yes.

The umask defines the mask for permissions with which files or directories are created using FTP. If file_umask is set to 177, then new files are created as having permissions 600, which defines rw———. The owner of this file has read and write permissions to this file, members in the users group do not have read/write permissions.

The server stop command terminates any existing FTP sessions.

### 8.1.3 OPTIONS

**bandwidth**  Upload or download bandwidth in Bytes/sec.

**nodename**  Node on which the operation takes place. A value of all indicates that the operation takes place on all nodes in the cluster.

**connections_number**  This is an integer, between 1 to 9999. This value defines the maximum number of simultaneous connections allowed for each node.

**port_range**  The port_range specifies a range of ports represented as startingport:endingport, both inclusive. The value of port numbers used should range from 30000 to 50000.

**time_in_minutes**  The value of time_in_minutes should range from 1 to 600. The time_in_minutes defines the amount of idle time after which a session is disconnected.

**login_directory**  The directory into which anonymous users login. The value of login_directory starts with /vx/.

**home_directory_path**  The directory in which user's directory should be created manually. The value of home_directory_path starts with /vx/.

**session_id**  The unique identifier for each FTP session. It is the value that is shown in session showdetail.

**filter_options**  Filters the sessions shown in session showdetail. Filter options include client_ip, server_ip, and user. Filter options can be combined by using ‘,’. If multiple filter options are used, sessions matching all the filter options are shown.

**server start|stop|status**  Start, stop, or display the status of the FTP server. All configuration changes made using the set command come into effect only when the server is restarted. For example, set command can be used to set the max_connections to 9999, but changes take effect only when the FTP server is restarted using server stop followed by server start. server stop terminates all existing FTP connections.

**set listen_port port_number**  This option specifies the port number on which the FTP service should listen for connections. Valid values for this parameter range from 10 to 1023. The default value of this parameter is 21. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

**set listen_ipv6 yes|no**  This option specifies if the FTP service should listen on IPv6 for connections. The default value of this parameter is no. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

**set max_connections connections_number**  This command specifies the maximum number of simultaneous FTP clients allowed per node. The default value of this parameter is 2000. Valid values for this parameter range from 1 to 9999. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.
set max_conn_per_client connections_number This option specifies the maximum number of simultaneous FTP connections allowed per client IP per server node. Valid values for this parameter range from 1 to 9999. The default value of this parameter is 2000. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set passive_port_range port_range This command specifies the range of port numbers to listen on for passive FTP transfers. The port_range defines a range specified as starting:portendingport. For example, a port_range of 30000:40000 specifies that port numbers starting from 30000 to 40000 can be used for passive FTP. Valid values for port numbers range from 30000 to 50000. The default value of this option is 30000:40000. These changes take effect when the FTP server is restarted using server stop followed by server start.

set idle_timeout time_in_minutes This command specifies the amount of time in minutes after which an idle connection is disconnected. Valid values for time_in_minutes range from 1 to 600. Default value for time_in_minutes is 15 minutes. These changes take effect when the FTP server is restarted using server stop followed by server start.

set allow_non_ssl yes|no This command specifies whether or not to allow non-secure (plain-text) logins into the FTP server. Entering yes allows non-secure (plain-text) logins to succeed. Entering no causes non-secure (plain-text) logins to fail. The default value for this parameter is yes. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set umask file_umask The umask defines the mask for permissions with which files or directories are created using FTP. If file_umask is set to 177, then new files are created as having permissions 600, which defines rw———. The owner of this file has read and write permissions to this file, members in the users group do not have read/write permissions. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set anonymous_logon yes|no This tells the FTP server whether or not to allow anonymous logins to the FTP server. Entering yes allows anonymous access to the FTP server. Entering no does not allow anonymous access. The default value of this parameter is no. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set anonymous_login_dir login_directory This command specifies the login directory of anonymous users. Valid values of this parameter start with /vx/. The administrator must ensure that the anonymous user (UID:40 GID:49 UNAME:ftp) has appropriate permissions to read files in login_directory. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set anonymous_write yes|no This command specifies whether or not anonymous users have write access in their login directory. Enter yes to allow anonymous users to modify contents of their login directory. A value of no does not allow anonymous users to modify contents of their login directory. The administrator must ensure that anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to modify files in login_directory. The default value of this parameter is no. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set user_logon yes|no This command specifies whether to allow FTP access for users. A value of yes would allow normal users (non-anonymous) to login. The default value of this parameter is yes. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set homedir_path login_directory This option specifies the login directory of normal users. Valid values of this parameter start with /vx/. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

set allow_delete yes|no This option specifies whether users are allowed to delete files on the FTP server. A value of yes allows users to delete uploaded files. This option only affects users and does
not affect anonymous logins. Anonymous logins are never allowed to delete files. The default value of this parameter is **yes**. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set security nis_ldap|ads|local** This option specifies what kind of users are allowed to login to the FTP server. A value of `nis_ldap` allows users configured on NIS or an LDAP server to login to the FTP server, and users created using `local user` or from Windows active directory are not allowed to login. A value of `ads` allows users configured on Windows active directory as specified in `cifs show`, NIS/LDAP, and `local user` users are not allowed to login. A value of `local` allows users created using `local user` to login to the FTP server, and NIS/LDAP/AD users are not allowed to login. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set chroot_users yes|no** This option specifies whether users should be restricted to their home directories. A value of `yes` limits users to his home directory. A value of `no` allows users to view files in parent directories, user is still restricted in `homedir_path`. If `security` is `local`, then `chroot_users` should be `yes`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set create_homedirs yes|no** This option specifies if home directories should be created when a user logs in, if it does not exist. A value of `yes` allows the FTP server to create the user's home directory, if it does not exist. If this is set to `no`, then there should already be a home directory created for this user, and the user should have permissions to read/execute in this directory, otherwise the login fails. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**show** Displays the list of all configurable options and their values. Use the `set` command to modify these values.

**session show** Displays the number of current FTP sessions for each node.

**session showdetail [filter_options]** Displays the details of the current FTP sessions.

**session terminate session_id** Terminates the FTP session using the session id.

**logupload url [nodename]** Uploads FTP logs to the URL `url`. The `url` supports FTP and SCP. If the `nodename` is specified, only logs from the `nodename` are uploaded. The default name for the uploaded file is `ftp_log.tar.gz`. Passwords added directly to the `url` are not supported.

**local user add username** Add a local FTP user with name `username`. This user gets authenticated when security is set to local. This command prompts for a password to be set for this user. The default home-directory for a user is the same as the `username`. Users created using this command can only access the files in their home directory and cannot see files of other users. Username can contain up to 32 characters.

**local user passwd username** Change password for the local FTP user with name `username`.

**local user delete username** Delete the `username` of the FTP user. This does not delete the `username`'s home directory. Home directory for `username` still continues to exist after deletion of the user.

**local user show** Show the list of users and information associated with the users.

**local user set bandwidth username bandwidth** Set the bandwidth for `username` to `bandwidth`. By default, there is no limit on the upload/download bandwidth limit for users. `bandwidth` is specified in Bytes/sec. Changes to this value are applicable for any new connections. If `bandwidth` is 0, then `bandwidth` is reset to unlimited bandwidth.

**local user set max_connections username number** Set the maximum number of simultaneous connections `username` can have to each node in the cluster to `number`. By default, there is no limit on the number of connections a user can have to the FTP server. Changes to this value are
applicable for any new connections. If number is 0, then max_connections is reset to unlimited connections.

**local user set homedir username homedir** Set the home directory for username to homedir. This does not migrate any existing data from username’s current home directory to homedir. homedir is relative to homedir_path that is set using set homedir_path. Changes to this value are applicable for any new connections.

### 8.1.4 EXAMPLES

Start the FTP server.

```
FTP> server start
```

View the current status of the FTP server.

```
FTP> server status
FTP Status on node_1 : ONLINE
FTP Status on node_2 : ONLINE
```

Stop the FTP server. (Terminates any existing FTP sessions.)

```
FTP> server stop
```

Display the current FTP server configuration.

```
FTP> show
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>max_connections</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>passive_port_range</td>
<td>30000:40000</td>
<td></td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>idle_timeout</td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
<td></td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftpanon</td>
<td></td>
</tr>
<tr>
<td>user_logon</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/ftphomes</td>
<td></td>
</tr>
<tr>
<td>allow_delete</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>security</td>
<td>local</td>
<td></td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
```

Change the maximum number of concurrent FTP connections allowed on the FTP server (restarting the FTP server will bring the changes into effect).

```
FTP> set max_connections 3000
Changes would be applicable after restart of FTP service.
Success.
```

```
FTP> show
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>----------------------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
</tbody>
</table>
```
listen_port  21
listen_ipv6  no
max_connections  2000  3000
max_conn_per_client  1000
passive_port_range  30000:40000
allow_non_ssl  yes
idle_timeout  15 minutes
umask  177
anonymous_logon  yes
anonymous_write  yes
anonymous_login_dir  /vx/ftp_fs/anon_dir
user_logon  no
homedir_path  /vx/ftp_fs/users_dir
allow_delete  yes
security  local
chroot_users  yes
create_homedirs  yes

FTP> server start
FTP> show
Parameter  Current Value
----------  ---------------
listen_port  21
listen_ipv6  no
max_connections  3000
max_conn_per_client  1000
passive_port_range  30000:40000
allow_non_ssl  yes
idle_timeout  15 minutes
umask  177
anonymous_logon  yes
anonymous_write  yes
anonymous_login_dir  /vx/ftp_fs/anon_dir
user_logon  no
homedir_path  /vx/ftp_fs/users_dir
allow_delete  yes
security  local
chroot_users  yes
create_homedirs  yes

Display the number of current FTP sessions.

    FTP> session show
Max Sessions : 2000

Nodename  Current Sessions
--------  ----------------
node_1  4
node_2  2

To view the details of all the current FTP sessions.

    FTP> session showdetail

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User</th>
<th>Client IP</th>
<th>Server IP</th>
<th>State</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_1.1111</td>
<td>user1</td>
<td>10.209.105.219</td>
<td>10.209.105.111</td>
<td>IDLE</td>
<td></td>
</tr>
<tr>
<td>node_1.1112</td>
<td>user2</td>
<td>10.209.106.11</td>
<td>10.209.105.111</td>
<td>IDLE</td>
<td></td>
</tr>
<tr>
<td>node_2.1113</td>
<td>user3</td>
<td>10.209.107.21</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
</tbody>
</table>
Upload the logs from all of the nodes to an SCP-based URL.

```
FTP> logupload scp://user@host:/path/to/directory
Password:
Collecting FTP logs, please wait.....
Uploading the logs to scp://user@host:/path/to/directory, please wait...done
```

Upload the logs from node_1 to an FTP-based URL.

```
FTP> logupload ftp://user@host:/path/to/directory node_1
Password:
Collecting FTP logs, please wait.....
Uploading the logs to ftp://user@host:/path/to/directory, please wait...done
```

### 8.1.5 SEE ALSO

server(1), show(1), set(1), session(1), logupload(1), local(1)
8.2 local

8.2.1 SYNOPSIS

local user add username
local user passwd username
local user delete username
local user show
local user set bandwidth username bandwidth
local user set max_connections username number
local user set homedir username homedir

8.2.2 DESCRIPTION

The local commands add, delete, or display FTP users. Local users’ home directories are automatically created when they login for the first time.

8.2.3 OPTIONS

*bandwidth*  Upload or download bandwidth in Bytes/sec.

local user add username  Add a local FTP user with name *username*. This user gets authenticated when security is set to local. This command prompts for a password to be set for this user. The default home directory for a user is the same as the *username*. Users created using this command can only access the files in their home directory and cannot see files of other users. *Username* can contain up to 32 characters.

local user passwd username  Change password for the local FTP user with name *username*.

local user delete username  Delete the *username* FTP user. This does not delete the *username*’s home directory. Home directory for *username* still continues to exist after deletion of the user.

local user show  Show the list of users and information associated with the users.

local user set bandwidth username bandwidth  Set the bandwidth for *username* to *bandwidth*. By default, there is no limit on upload/download bandwidth limit for users. *bandwidth* is specified in Bytes/sec. Changes to this value are applicable for any new connections. If *bandwidth* is 0, then download_bandwidth is reset to unlimited bandwidth.

local user set max_connections username number  Set the maximum number of simultaneous connections *username* can have to each node in the cluster to *number*. By default, there is no limit on the number of connections a user can have to the FTP server. Changes to this value are applicable for any new connections. If *number* is 0, then max_connections is reset to unlimited connections.

local user set homedir username homedir  Set the home directory for *username* to *homedir*. This does not migrate any existing data from the *username*’s current home directory to *homedir*. *homedir* is relative to homedir_path that is set using set homedir_path. Changes to this value are applicable for any new connections.
8.2.4 EXAMPLES

Adds a local FTP user localuser1.

```
FTP> local user add localuser1
Input password for localuser1.
Enter password:
Re-enter password:
Success.
```

Changes the password for user localuser1.

```
FTP> local user passwd localuser1
Input password for localuser1.
Enter password:
Re-enter password:
Success.
```

Deletes user localuser1.

```
FTP> local user delete localuser1
Success.
```

Show the list of local FTP users.

```
FTP> local user show
USER HOMEDIR BANDWIDTH MAX_CONN
---- ------- -------- ---------
localuser1 /localuser1 - 10
localuser2 /localuser2 2046 -
localuser3 /localuser3 - -
localuser4 /localuser4 - -
```

Changes the maximum number of simultaneous connections localuser3 can have to any node in the cluster to 200.

```
FTP> local user set max_connections localuser3 200
Success.
```

```
FTP> local user show
USER HOMEDIR BANDWIDTH MAX_CONN
---- ------- -------- ---------
localuser1 /localuser1 - 10
localuser2 /localuser2 2046 -
localuser3 /localuser3 - 200
localuser4 /localuser4 - -
```

Changes the home directory of localuser4 /localuser4_new.

```
FTP> local user set homedir localuser3 /localuser4_new
Success.
```

```
FTP> local user show
USER HOMEDIR BANDWIDTH MAX_CONN
---- ------- -------- ---------
localuser1 /localuser1 - 10
localuser2 /localuser2 2046 -
localuser3 /localuser3 - 200
localuser4 /localuser4_new - -
```
8.2.5 SEE ALSO

server(1), set(1)
8.3 logupload

8.3.1 SYNOPSIS

logupload url [nodename]

8.3.2 DESCRIPTION

The logupload command allows the user to upload the FTP server logs to url. The default name for the uploaded file is ftp_log.tar.gz.

8.3.3 OPTIONS

- **nodename** The node on which the operation occurs. A value of all indicates the operation takes place on all of the nodes in the cluster.

- **logupload url [nodename]** Uploads FTP logs to the URL url. The url supports FTP and SCP. If nodename is specified, only logs from the node nodename are uploaded. The default name for the uploaded file is ftp_log.tar.gz. Passwords added directly to the url are not supported.

8.3.4 EXAMPLES

To upload the logs from all of the nodes to an SCP-based URL.

```
FTP> logupload scp://user@host:/path/to/directory
Password:
Collecting FTP logs, please wait....
Uploading the logs to scp://user@host:/path/to/directory, please wait...done
```

To upload the logs from node_1 to an FTP-based URL.

```
FTP> logupload ftp://user@host:/path/to/directory node_1
Password:
Collecting FTP logs, please wait.....
Uploading the logs to ftp://user@host:/path/to/directory, please wait...done
```

8.3.5 SEE ALSO

server(1), show(1), set(1), session(1)
8.4 server

8.4.1 SYNOPSIS

server [start|stop|status]

8.4.2 DESCRIPTION

The FTP server command starts, stops, or checks the status of the FTP server. The server stop command terminates any existing FTP sessions.

8.4.3 OPTIONS

server [start|stop|status] Start, stop, or check the status of the FTP server.

8.4.4 EXAMPLES

Start the FTP server. If the FTP server is already started, Veritas Access clears the faults (if any), and then tries to start the FTP server.

```
FTP> server start
Success.
FTP> server status
FTP Status on node_1 : ONLINE
FTP Status on node_2 : ONLINE
```

Stop the FTP server. Terminates any existing FTP sessions.

```
FTP> server stop
Success.
FTP> server status
FTP Status on node_1 : OFFLINE
FTP Status on node_2 : OFFLINE
```

8.4.5 SEE ALSO

set(1), show(1), session(1), logupload(1)
8.5 session

8.5.1 SYNOPSIS

```bash
session show
session showdetail [filter_options]
session terminate session_id
```

8.5.2 DESCRIPTION

The `session` commands allow the user to view or terminate the current FTP sessions to the server.

8.5.3 OPTIONS

- **session_id** The unique identifier for each FTP session. It is the value that is displayed in `session showdetail`.

- **filter_options** The `filter_options` filter the sessions displayed in `session showdetail`. Filter options include client_ip, server_ip, and user. Filter options can be combined by using ','. If multiple filter options are used, sessions matching all of the filter options are displayed.

- **session show** Displays the number of current FTP sessions on each node.

- **session showdetail [filter_options]** Displays the details of each session that matches the `filter_options` criteria. If no `filter_options` is specified, all the sessions are displayed. If multiple filter options are provided, then sessions matching all the filter options are displayed. For each session, user, client IP, server IP, session state (Uploading/Downloading/Idle), file (uploading/downloading file) is displayed. A value of '?' for the user signifies the session is not authenticated yet.

- **session terminate session_id** Terminates the session with the session ID as `session_id`. The `session_id` is the value displayed in `session showdetail`.

8.5.4 EXAMPLES

To view the number of current FTP sessions.

```bash
FTP> session show
Max Sessions : 2000
Nodename Current Sessions
-------- ----------------
node_1  4
node_2  2
```

To view the details of all the current FTP sessions.

```bash
FTP> session showdetail
Session ID User     Client IP          Server IP          State  File
-------- ------:-------:----------:----------:------:------
node_1.1111 user1    10.209.105.219 10.209.105.111 IDLE
node_1.1112 user2    10.209.106.11  10.209.105.111 IDLE
node_2.1113 user3    10.209.107.21  10.209.105.112 IDLE
node_1.1117 user4    10.209.105.219 10.209.105.111 DL file123
```
To view the details of the current FTP sessions originating from client 10.209.107.21.

```
FTP> session showdetail client_ip=10.209.107.21
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User</th>
<th>Client IP</th>
<th>Server IP</th>
<th>State</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_2.1113</td>
<td>user3</td>
<td>10.209.107.21</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
</tbody>
</table>

To view the details of the current FTP sessions to the server IP 10.209.105.112.

```
FTP> session showdetail server_ip=10.209.105.112
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User</th>
<th>Client IP</th>
<th>Server IP</th>
<th>State</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_2.1113</td>
<td>user3</td>
<td>10.209.107.21</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
<tr>
<td>node_1.1121</td>
<td>user5</td>
<td>10.209.111.219</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
</tbody>
</table>

To view the details of the current FTP sessions to the server IP 10.209.105.112 originating from client 10.209.107.21.

```
FTP> session showdetail server_ip=10.209.105.112,client_ip=10.209.107.21
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User</th>
<th>Client IP</th>
<th>Server IP</th>
<th>State</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_2.1113</td>
<td>user3</td>
<td>10.209.107.21</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
</tbody>
</table>

To view the details of the current FTP sessions to the server IP 10.209.105.112 by user user3.

```
FTP> session showdetail server_ip=10.209.105.112,user=user3
```

<table>
<thead>
<tr>
<th>Session ID</th>
<th>User</th>
<th>Client IP</th>
<th>Server IP</th>
<th>State</th>
<th>File</th>
</tr>
</thead>
<tbody>
<tr>
<td>node_2.1113</td>
<td>user3</td>
<td>10.209.107.21</td>
<td>10.209.105.112</td>
<td>IDLE</td>
<td></td>
</tr>
</tbody>
</table>

To terminate a FTP session that is displayed in session showdetail.

```
FTP> session terminate node_2.1113
```

Session node_2.1113 terminated

### 8.5.5 SEE ALSO

server(1), show(1), set(1), logupload(1)
8.6 set

8.6.1 SYNOPSIS

set listen_port port_number
set listen_ipv6 yes|no
set max_connections connections_number
set max_conn_per_client connections_number
set passive_port_range port_range
set idle_timeout time_in_minutes
set allow_non_ssl yes|no
set umask file_umask
set anonymous_logon yes|no set anonymous_login_dir login_directory set anonymous_write yes|no
set user_logon yes|no set homedir_path home_directory_path set allow_delete yes|no set security nis ldaps|local set chroot_users yes|no set create_homedirs yes|no

8.6.2 DESCRIPTION

The set commands allow the user to set various configurable options for the FTP server.

8.6.3 OPTIONS

- **login_directory** Login directory is the directory into which users login. The value of login_directory starts with /vx.

- **home_directory_path** The directory in which users home directories are created. The value of home_directory_path starts with /vx/.

- **connections_number** This is an integer, with a range between 1 to 9999. This value defines the maximum number of simultaneous connections allowed for each node.

- **port_range** The port_range specifies a range of ports represented as startingport:endingport. Both ports are inclusive. The port numbers use a range from 30000 to 50000.

- **time_in_minutes** Values for time_in_minutes range from 1 to 600. The time_in_minutes defines the amount of idle time after which a session is disconnected.

- **set listen_port port_number** This option specifies the port number on which the FTP service should listen for connections. Valid values for this parameter range from 10 to 1023. The default value of this parameter is 21. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

- **set listen_ipv6 yes|no** This option specifies if the FTP service should listen on IPv6 connections. The default value of this parameter is no. Changes to this value take effect when the FTP server is restarted using server stop followed by server start.

- **set max_connections connections_number** This command specifies the maximum number of simultaneous FTP clients allowed per node. The default value of this parameter is 2000. Valid values
for this parameter range from 1 to 9999. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set max_conn_per_client connections_number** This option specifies the maximum number of simultaneous FTP connections allowed per client IP per server node. Valid values for this parameter range from 1 to 9999. The default value of this parameter is 2000. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set passive_port_range port_range** This command specifies the range of port numbers to listen on for passive FTP transfers. The `port_range` defines a range specified as `startingport:endingport`. For example, a `port_range` of `30000:40000` specifies that port numbers starting from 30000 to 40000 can be used for passive FTP. Valid values for `port_range` range from 30000 to 50000. The default value of this option is `30000:40000`. These changes take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set idle_timeout time_in_minutes** This command specifies the amount of time in minutes after which an idle connection is disconnected. Valid values for `time_in_minutes` range from 1 to 600. The default value for `time_in_minutes` is 15 minutes. These changes take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set allow_non_ssl yes|no** This command specifies whether or not to allow non-secure (plain-text) logins into the FTP server. Entering `yes` allows non-secure (plain-text) logins to succeed. Entering `no` causes non-secure (plain-text) logins to fail. The default value for this parameter is `yes`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set umask file_umask** The `umask` defines the mask for permissions with which files or directories are created using FTP. If `file_umask` is set to 177, then new files are created as having permissions 600, which defines `rw——–`. The owner of this file has read and write permissions to this file, members in the users group do not have read/write permissions. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set anonymous_logon yes|no** This tells the FTP server whether or not to allow anonymous logins to the FTP server. Entering `yes` allows anonymous users to login to the FTP server. Entering `no` does not allow anonymous logins. The default value of this parameter is `no`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set anonymous_login_dir login_directory** This command specifies the login directory of anonymous users. Valid values of this parameter start with `/vx/`. The administrator must ensure that the anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to read files in `login_directory`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set anonymous_write yes|no** This command specifies whether or not anonymous users can write to their login directory. Enter `yes` to allow anonymous users to modify contents of their `login_directory`. A value of `no` does not allow anonymous users to modify contents of their `login_directory`. The administrator must ensure that anonymous user (UID:40 GID:49 UNAME:ftp) has appropriate permissions to modify files in `login_directory`. The default value of this parameter is `no`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set user_logon yes|no** This command specifies whether to allow FTP access for users. A value of `yes` allows normal users(non-anonymous) to login. The default value of this parameter is `yes`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set homedir_path login_directory** This option specifies the login directory of normal users. Valid values of this parameter start with `/vx/`. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`. 
**set allow_delete yes|no** This option specifies whether users are allowed to delete files on the FTP server. A value of *yes* allows users to delete uploaded files. This option only affects users and does not affect anonymous logins. Anonymous logins are never allowed to delete files. The default value of this parameter is *yes*. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set security nis_ldap|ads|local** This option specifies what kind of users are allowed to login to the FTP server. A value of *nis_ldap* allows users configured on NIS or an LDAP server to login to the FTP server, and users created using *local user* or from Windows active directory are not allowed to login. A value of *ads* allows users configured on Windows active directory as specified in `cifs show`, NIS/LDAP and *local user* users are not allowed to login. A value of *local* allows users created using *local user* to login to the FTP server, and NIS/LDAP/AD users are not allowed to login. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set chroot_users yes|no** This option specifies whether users should be restricted to their home directories. A value of *yes* limits users to his home directory. A value of *no* will allow users to view files in parent directories, user will still be restricted of `homedir_path`. If `security` is *local*, then `chroot_users` should be *yes*. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

**set create_homedirs yes|no** This option specifies if home directories should be created when a user logs in, if it does not exist. A value of *yes* lets FTP create the user’s home directory, if it does not exist. If this is set to *no*, then there should already be a home directory created for this user and the user should have permissions to read/execute in this directory, otherwise the login fails. Changes to this value take effect when the FTP server is restarted using `server stop` followed by `server start`.

### 8.6.4 EXAMPLES

Allows anonymous logins to the FTP server. Restart the FTP server to bring the changes into effect.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>max_connections</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>passive_port_range</td>
<td>30000:40000</td>
<td></td>
</tr>
<tr>
<td>idle_timeout</td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
<td></td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftpanon</td>
<td></td>
</tr>
<tr>
<td>user_logon</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/ftphomes</td>
<td></td>
</tr>
<tr>
<td>allow_delete</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>security</td>
<td>local</td>
<td></td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter     Current Value
-----------  -------------------
listen_port   21
listen_ipv6   no
max_connections  2000
max_conn_per_client  1000
passive_port_range  30000:40000
idle_timeout     15 minutes
allow_non_ssl    yes
umask           177
anonymous_logon yes
anonymous_write no
anonymous_login_dir /vx/ftpanon
user_logon       yes
homedir_path     /vx/ftphomes
allow_delete     yes
security         local
chroot_users     yes
create_homedirs  yes

Allows anonymous users to have write permissions to their login directory on the FTP server. Restart the FTP server to bring the changes into effect.

FTP> set anonymous_write yes
Changes would be applicable after restart of FTP service.
Success.

FTP> show
Parameter     Current Value     New Value
-----------  ---------------------  --------
listen_port   21                   
listen_ipv6   no                    
max_connections  2000                
max_conn_per_client  1000            
passive_port_range  30000:40000      
idle_timeout     15 minutes          
allow_non_ssl    yes                 yes
umask           177                 177
anonymous_logon yes                 yes
anonymous_write no                 yes
anonymous_login_dir /vx/ftpanon     /vx/ftpanon
user_logon       yes                yes
homedir_path     /vx/ftphomes       /vx/ftphomes
allow_delete     yes                yes
security         local               local
chroot_users     yes                yes
create_homedirs  yes                yes

FTP> server stop
Success.

8.6. set
FTP> server start
Success.

FTP> show
Parameter Current Value
--------- -------------
listen_port 21
listen_ipv6 no
max_connections 2000
max_conn_per_client 1000
passive_port_range 30000:40000
idle_timeout 15 minutes
allow_non_ssl yes
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftpanon
user_logon yes
homedir_path /vx/ftphomes
allow_delete yes
security local
chroot_users yes
create_homedirs yes

Changes the login directory of the anonymous user on the FTP server. Restart the FTP server to bring the changes into effect.

FTP> set anonymous_login_dir /vx/ftp_fs/anon_dir
Changes would be applicable after restart of FTP service.
Success.

FTP> show
Parameter Current Value New Value
--------- -------------- ---------
listen_port 21
listen_ipv6 no
max_connections 2000
max_conn_per_client 1000
passive_port_range 30000:40000
idle_timeout 15 minutes
allow_non_ssl yes
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftpanon /vx/ftp_fs/anon_dir
user_logon yes
homedir_path /vx/ftphomes
allow_delete yes
security local
chroot_users yes
create_homedirs yes

FTP> server stop
Success.

FTP> server start
Success.
FTP> show
Parameter Current Value
--------- -----------
listen_port 21
listen_ipv6 no
max_connections 2000
max_conn_per_client 1000
passive_port_range 30000:40000
idle_timeout 15 minutes
allow_non_ssl yes
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon yes
homedir_path /vx/ftphomes
allow_delete yes
security local
chroot_users yes
create_homedirs yes

Allows only anonymous access to the FTP server, user access is denied. Restart the FTP server to bring the changes into effect.

FTP> set user_logon no
Changes would be applicable after restart of FTP service.
Success.

FTP> server start
Success.

FTP> show
Parameter Current Value
--------- -----------
listen_port 21
listen_ipv6 no
max_connections 2000
max_conn_per_client 1000
passive_port_range 30000:40000
idle_timeout 15 minutes
allow_non_ssl yes
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon no
homedir_path /vx/ftphomes
allow_delete yes
security local
chroot_users yes
create_homedirs yes

Changes the login directory of the normal user (non-anonymous users) on the FTP server. Restart the FTP server to bring the changes into effect.

8.6. set
FTP> set homedir_path /vx/ftp_fs/users_dir
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.
FTP> server start
Success.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
</tr>
<tr>
<td>max_connections</td>
<td>2000</td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>1000</td>
</tr>
<tr>
<td>passive_port_range</td>
<td>30000:40000</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>15 minutes</td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>yes</td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftp_fs/anon_dir</td>
</tr>
<tr>
<td>user_logon</td>
<td>no</td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/ftp_fs/users_dir</td>
</tr>
<tr>
<td>allow_delete</td>
<td>yes</td>
</tr>
<tr>
<td>security</td>
<td>local</td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
</tr>
</tbody>
</table>

Changes the maximum number of concurrent FTP connections allowed on the FTP server. Restart the FTP server to bring the changes into effect.

FTP> set max_connections 3000
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
</tr>
<tr>
<td>max_connections</td>
<td>3000</td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>1000</td>
</tr>
<tr>
<td>passive_port_range</td>
<td>30000:40000</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>15 minutes</td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>yes</td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftp_fs/anon_dir</td>
</tr>
<tr>
<td>user_logon</td>
<td>no</td>
</tr>
</tbody>
</table>
Changes the maximum number of concurrent FTP connections allowed to the FTP server from a client IP. Restart the FTP server to bring the changes into effect.

```
FTP> set max_conn_per_client 500
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter Current Value
--------- ---------------
listen_port 21
listen_ipv6 no
max_connections 3000
max_conn_per_client 500
passive_port_range 30000:40000
idle_timeout 15 minutes
allow_non_ssl yes
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon no
homedir_path /vx/ftp_fs/users_dir
allow_delete yes
security local
chroot_users yes
create_homedirs yes
```

Allows only secure (SSL) logins and rejects plain-text logins. Restart the FTP server to bring the changes into effect.

```
FTP> set allow_non_ssl no
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter Current Value
--------- ---------------
listen_port 21
listen_ipv6 no
max_connections 3000
```
Changes the passive port range to 35000:45000. Restart the FTP server to bring the changes into effect.

```
FTP> set passive_port_range 35000:45000
Changes would be applicable after restart of FTP service.
Success.
```

```
FTP> server stop
Success.
```

```
FTP> server start
Success.
```

```
FTP> show
Parameter Current Value
--------- ------------
listen_port 21
listen_ipv6 no
max_connections 3000
max_conn_per_client 500
passive_port_range 35000:45000
idle_timeout 15 minutes
allow_non_ssl no
anonymous_logon yes
umask 177
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon no
homedir_path /vx/ftp_fs/users_dir
allow_delete yes
security local
chroot_users yes
create_homedirs yes
```

Changes the idle timeout value to 300. Restart the FTP server to bring the changes into effect.

```
FTP> set idle_timeout 300
Changes would be applicable after restart of FTP service.
Success.
```

```
FTP> server stop
Success.
```
FTP> server start
Success.

FTP> show
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
</tr>
<tr>
<td>max_connections</td>
<td>3000</td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>500</td>
</tr>
<tr>
<td>passive_port_range</td>
<td>35000:45000</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>300 minutes</td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>no</td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftp_fs/anon_dir</td>
</tr>
<tr>
<td>user_logon</td>
<td>no</td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/ftp_fs/users_dir</td>
</tr>
<tr>
<td>allow_delete</td>
<td>yes</td>
</tr>
<tr>
<td>security</td>
<td>local</td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
</tr>
</tbody>
</table>

Changes the write access to users to deny delete operations. Restart the FTP server to bring the changes into effect.

FTP> set allow_delete no
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
</tr>
<tr>
<td>max_connections</td>
<td>3000</td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>500</td>
</tr>
<tr>
<td>passive_port_range</td>
<td>35000:45000</td>
</tr>
<tr>
<td>idle_timeout</td>
<td>300 minutes</td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>no</td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/ftp_fs/anon_dir</td>
</tr>
<tr>
<td>user_logon</td>
<td>no</td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/ftp_fs/users_dir</td>
</tr>
<tr>
<td>allow_delete</td>
<td>no</td>
</tr>
<tr>
<td>security</td>
<td>local</td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
</tr>
</tbody>
</table>
Changes the port on which FTP service will listen for incoming connections. Restart the FTP server to bring the changes into effect.

```
FTP> set listen_port 24
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter Current Value
--------- -------------
listen_port 24
listen_ipv6 no
max_connections 3000
max_conn_per_client 500
passive_port_range 35000-45000
idle_timeout 300 minutes
allow_non_ssl no
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon no
homedia_path /vx/ftp_fs/users_dir
allow_delete no
security local
chroot_users yes
create_homdirs yes
```

Changes the users’ database from local to NIS/LDAP. Restart the FTP server to bring the changes into effect.

```
FTP> set security nis_ldap
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter Current Value
--------- -------------
listen_port 24
listen_ipv6 no
max_connections 3000
max_conn_per_client 500
passive_port_range 35000-45000
idle_timeout 300 minutes
allow_non_ssl no
umask 177
anonymous_logon yes
anonymous_write yes
```
Allows users to read parent directories of their home directories. Restart the FTP server to bring the changes into effect.

```
FTP> set chroot_users no
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter          Current Value
-------             -------------
listen_port        24
listen_ipv6        no
max_connections    3000
max_conn_per_client 500
passive_port_range 35000:45000
idle_timeout       300 minutes
allow_non_ssl      no
umask              177
anonymous_logon    yes
anonymous_write    yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon         no
homedir_path       /vx/ftp_fs/users_dir
allow_delete       no
security           nis_ldap
chroot_users       no
create_homedirs    yes
```

Do not automatically create home directories for users when they login. Restart the FTP server to bring the changes into effect.

```
FTP> set create_homedirs no
Changes would be applicable after restart of FTP service.
Success.

FTP> server stop
Success.

FTP> server start
Success.

FTP> show
Parameter          Current Value
-------             -------------
8.6. set
```
listen_port 24
listen_ipv6 no
max_connections 3000
max_conn_per_client 500
passive_port_range 35000:45000
idle_timeout 300 minutes
allow_non_ssl no
umask 177
anonymous_logon yes
anonymous_write yes
anonymous_login_dir /vx/ftp_fs/anon_dir
user_logon no
homedir_path /vx/ftp_fs/users_dir
allow_delete no
security nis_ldap
chroot_users no
create_homedirs no

8.6.5 SEE ALSO

server(1), show(1), local(1)
8.7 show

8.7.1 SYNOPSIS

show

8.7.2 DESCRIPTION

The show command displays the list of all the configurable options and their values. These are the settings that have been configured primarily with the set command.

8.7.3 EXAMPLES

Display the current FTP server configuration.

```
FTP> show

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Current Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen_port</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>listen_ipv6</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>max_connections</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>max_conn_per_client</td>
<td>2000</td>
<td></td>
</tr>
<tr>
<td>passive_port_range</td>
<td>30000:40000</td>
<td></td>
</tr>
<tr>
<td>allow_non_ssl</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>idle_timeout</td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td>umask</td>
<td>177</td>
<td></td>
</tr>
<tr>
<td>anonymous_logon</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>anonymous_write</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>anonymous_login_dir</td>
<td>/vx/fs_1</td>
<td></td>
</tr>
<tr>
<td>user_logon</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>homedir_path</td>
<td>/vx/fs_1_test</td>
<td></td>
</tr>
<tr>
<td>allow_delete</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>security</td>
<td>local</td>
<td></td>
</tr>
<tr>
<td>chroot_users</td>
<td>yes</td>
<td></td>
</tr>
<tr>
<td>create_homedirs</td>
<td>yes</td>
<td></td>
</tr>
</tbody>
</table>
```

8.7.4 SEE ALSO

set(1), server(1), session(1), logupload(1)
9.1 network

9.1.1 SYNOPSIS

ping destination [nodename] [devicename] [packets]
dns show
dns enable
dns disable
firewall status
firewall enable
firewall disable
dns set domainname domainname
dns set nameservers nameserver1 [nameserver2] [nameserver3]
dns clear domainname
dns clear nameservers
show
nis show [users|groups|netgroups]
nis disable
nis enable
nis set servername servername
nis set domainname [domainname]
nsswitch show
nsswitch conf { group|hosts|netgroup|passwd|shadow }

  value1 value2 value3
ip link set nodename device { up | down | mtu MTU }
ip link show [nodename] [device]
ip addr modify oldipaddr newipaddr { netmask | prefix }
ip addr del ipaddr
ip addr add ipaddr { netmask | prefix } type [device] [nodename]
ip addr online ipaddr nodename
ip addr show
ip route show [nodename]
ip route add nodename ipaddr { netmask | prefix } via gateway [dev device]
ip route del nodename ipaddr { netmask | prefix }
ldap enable
ldap disable
ldap show [users|groups|netgroups]
ldap set { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash } value
ldap get { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash }
bond show
bond create interfacelist mode
bond remove bondname
netgroup add groupname memberlist
netgroup delete groupname [memberlist]
netgroup show [groupname]
vlan show
vlan add device vlan_id
vlan del vlan_device
device add devicename
device remove devicename
device rename old_name with new_name nodename
device identify devicename nodename [timeout]
device list nodename
device ipmonitor add devicename ipaddress1 [, ipaddress2,...]
device ipmonitor del devicename
device ipmonitor show
swap interface1 interface2 [nodename]
pciexclusion show
9.1.2 DESCRIPTION

These network commands are used to configure DNS, NIS, LDAP client, IP, and check the status.

9.1.3 OPTIONS

-pcieclusion add pci
-pcieclusion delete pci

krb standalone set kdc_server kerberos_realm keytab_file

krb standalone unset

krb standalone show

**ping** destination [nodename] [devicename] [packets] Test whether a particular host or gateway is reachable across an IP network.

**dns show** Display the current DNS settings. Shows whether DNS is enabled or disabled, and the current values for the domain name and name servers.

**dns enable** Enable DNS usage.

**dns disable** Disable DNS usage.

**firewall status** Display whether the current firewall status is enabled or disabled.

**firewall enable** Enable the firewall setting to allow specific IPs to connect to the ports while blocking other connections.

**firewall disable** Disable the firewall setting.

**dns set domainname** domainname Set the domain name of the server to domainname. To clear the domain name, use dns clear domainname.

**dns set nameservers** nameserver1 [nameserver2] [nameserver3] Modify the DNS name servers that are used. Specify the name servers in the order in which the name servers are to be used. Specify up to three name servers. To clear the name servers list, use the dns clear nameservers command.

**dns clear domainname** Clear the domain name used by DNS.

**dns clear nameservers** Clear the name servers list used by DNS.

**show** Display the network configuration and statistics on all the available nodes.

**nis show** Display the NIS server name and domain name.

**nis show users** Display NIS users that are available in the NIS database.

**nis show groups** Display NIS groups that are available in the NIS database.

**nis show netgroups** Display NIS netgroups that are available in the NIS database.

**nis disable** Disable the NIS clients on all the nodes.

**nis enable** Enable NIS clients on all the nodes.

**nis set servername** servername Set the NIS server name on all the nodes.

**nis set domainname [domainname]** Set the NIS domain name on all the nodes.

**nsswitch show** Display the name service switch configuration.
nsswitch conf { group|hosts|netgroup|passwd|shadow } value1 value2 value3 Configure the method for the name service switch lookup process.

ip link set nodename device { up | down | mtu MTU } Change device attributes. Use all to change the attributes on all nodes.

ip link show [nodename] [device] Display device attributes.

ip addr modify oldipaddr newipaddr { netmask | prefix } Modify an IP address used by the cluster.

ip addr del ipaddr Delete an IP address.

ip addr add ipaddr [ netmask | prefix ] type [ device ] [ nodename ] Add a new IP address.

ip addr online ipaddr nodename Bring an IP address used by the cluster online on any running node in the cluster.

ip addr show Display IP addresses and their properties.

ip route show [nodename] Display route entries in the routing table for the cluster.

ip route add nodename ipaddr { netmask | prefix } via gateway [ dev device ] Add a new route.

ip route del nodename ipaddr { netmask | prefix } Delete a route used by the cluster.

ldap enable Enable the LDAP client, and configure the Pluggable Authentication Module (PAM) configuration files to use LDAP.

ldap disable Disable the LDAP client, and configure PAM configuration files not to use LDAP.

ldap show Show the LDAP client configuration.

ldap show users Show LDAP users that are available in the NSS database.

ldap show groups Show LDAP groups that are available in the NSS database.

ldap show netgroups Show LDAP netgroups that are available in the NSS database.

ldap set server value Set the LDAP server’s host name or IP address. This setting is mandatory.

ldap set port value Set the LDAP server’s port. Default value is 389.

ldap set basedn value Set the LDAP base Distinguished Name (DN). This setting is mandatory.

ldap set ssl { on | off } Set LDAP over Secure Sockets Layer (SSL) on or off. Set to “on” if your LDAP server supports SSL. Certificates required for SSL are auto-negotiated with the LDAP server during session establishment. The default value is “off.” This setting is mandatory.

ldap set binddn value Set the LDAP bind DN and its password. This DN is used to bind with the LDAP server for read access. For authentication, read access to most of the attributes is required. This setting is mandatory.

ldap set rootbinddn value Set the LDAP root bind DN and its password. This DN is used to bind with the LDAP server for write access. This setting is not required for authentication. To change some attributes of an LDAP entry, this DN is required. For example, changing a user’s password by root (uid=0) user requires System Administrator privileges to write into the LDAP directory. This setting is optional.

ldap set users-basedn value Set the LDAP users base DN. This DN is used by the authentication system (PAM and NSS) to search LDAP users. This setting is mandatory.

ldap set groups-basedn value Set the LDAP groups base DN. This DN is used by the authentication system (PAM and NSS) to search the LDAP groups. This setting is mandatory.

ldap set netgroups-basedn value Set the LDAP netgroups base DN. This DN is used by the authentication system (PAM and NSS) to search the LDAP netgroups. This setting is mandatory.
**ldap set password-hash** {clear|crypt|md5} Set the password hash to use when setting an LDAP user’s password. The password will be encrypted with the configured hash algorithm before sending it to the LDAP server for storing into the LDAP directory. This setting is optional.

**ldap get** {server|port|basedn|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash} Get the values of the configured settings.

**bond show** Display the bond settings.

**bond create** interfacelist mode {0 | 1 | 2 | 3 | 4 | 5 | 6 | balance-rr | active-backup | balance-xor | broadcast | 802.3ad | balance-tlb | balance-alb} Create the bond of listed interfaces in a specified mode.

**bond remove** bondname Remove the bond configuration of given bondname.

**netgroup add** groupname memberlist Add members to an existing netgroup or create a new netgroup.

**netgroup delete** groupname [memberlist] Delete the members of an existing netgroup or delete whole netgroup.

**netgroup show** [groupname] Display the netgroup settings.

**vlan show** Display the current VLAN devices.

**vlan add** device vlan_id Add a VLAN device with interface device and VLAN id as vlan_id.

**vlan del** vlan_device Delete the VLAN device vlan_device.

**device add** devicename Add a NIC device devicename in cluster.

**device remove** devicename Remove NIC device devicename from cluster.

**device rename** old_name with new_name nodename Rename NIC device old_name with new_name on given node nodename of cluster.

**device identify** devicename nodename [timeout] Identify interface devicename by sight on given node nodename of cluster. Optional timeout can be specified. Default timeout is 120 sec.

**device list** nodename List all plugged NIC devices on node nodename.

**device ipmonitor add** devicename ipaddress1 [, ipaddress2,...] Add monitoring IP address(es) for public NIC devices.

**device ipmonitor del** devicename Delete the existing configuration of monitoring IP address(es) for a NIC device.

**device ipmonitor show** Display IP address(es) monitoring information for NIC devices.

**swap interface1 interface2 [nodename]** Swap two network interfaces on a node in the cluster.

**pciexclusion show** This command displays the PCI Id those have been provided for exclusion.

**pciexclusion add** [pci_list] This commands allows administrator to add specific PCI BusId(s) for exclusion. These values must be provided before doing installation, then only it enables to exclude PCI from second node installation.

**pciexclusion delete** [pci] This commands allows administrator to delete given PCI Id from exclusion. This command must be used before doing installation then only it takes effect.

**krb standalone set** kdc_server kerberos_realm keytab_file This command is used to enable Kerberos authentication for NFS on Veritas Access.

**krb standalone show** Display the Kerberos configuration.

**krb standalone unset** Reset the Kerberos configuration.
9.1.4 SEE ALSO

bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1), krb(1)
9.2 bond

9.2.1 SYNOPSIS

bond show
bond create interfaceList mode
bond remove bondname
bond private-links-create
bond private-links-remove

9.2.2 DESCRIPTION

The bond command is used to view, create, or remove the bonding of Ethernet interfaces.

9.2.3 OPTIONS

interfaceList InterfaceList is the comma-separated list of public devices to be bonded.
mode Bonding of Ethernet interfaces can be done with the following types of modes
balance-rr or 0 Transmit packets in sequential order from the first available slave through the last. This
mode provides load balancing and fault tolerance.: active-backup or 1 Only one slave in the bond is active. A different slave becomes active if, and only
if, the active slave fails. The bond’s MAC address is externally visible on only one port (Ethernet
interface) to avoid confusing the switch.
balance-xor or 2 Transmit based on the selected transmit hash policy. The default policy is a simple
[(source MAC address XOR’d with destination MAC address) modulo slave count]. Alternate trans-
mit policies may be selected via the xmit_hash_policy option. This mode provides load balancing
and fault tolerance.
broadcast or 3 Transmits everything on all slave interfaces. This mode provides fault tolerance.
802.3ad or 4 Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves
in the active aggregator according to the 802.3ad specification.: balance-tlb or 5 Channel bonding that does not require any special switch support. The outgoing traffic
is distributed according to the current load (computed relative to the speed) on each slave. Incoming
traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC
address of the failed receiving slave.
balance-alb or 6 Includes balance-tlb plus receive load balancing (RLB) for IPV4 traffic, and does not
require any special switch support. The receive load balancing is achieved by ARP negotiation.: bond show Show the current bonding settings.
bond create interfaceList mode Create the bond of devices given as interfaceList, in a given mode.
During bond creation, ssh connection may be disconnected. The MTU of a bond in-
terface is calculated as minimum of the MTUs of the bonded interfaces.
bond remove bondname Remove the bonding of Ethernet interfaces for the given bondname. During
bond remove, ssh connection may be disconnected.
bond priv-create  Create the bond for the private interfaces (priveth0 & priveth1) with mode 0 (balance-rr). Veritas Access supports only mode 0 for the private interfaces. During bond creation, Veritas Access will offline all service groups, and you will need to run this command using the server console. The MTU of a bond interface is calculated as minimum of the MTUs of the bonded interfaces.

bond priv-remove  Remove the bonding of private interfaces (priveth0 & priveth1) for the cluster. During bond remove, Veritas Access will offline all service groups, and you will need to run this command using server console.

9.2.4 EXAMPLES

Display the bond settings.

```
Network> bond show
BONDNAME  MODE     DEVICES
--------    -------
bond0      active-backup  pubeth1 pubeth2

Network> bond show
BONDNAME  MODE     DEVICES
--------    -------
privbond0  balance-rr  priveth0 priveth1
```

Create the bond of the devices given as interfaceList in a specified mode.

```
Network> bond create pubeth1,pubeth2 1
100% [#] Bonding interfaces. Please wait...
bond created, the bond name is: bond0
```

Remove the bond settings of the entered bondname.

```
Network> bond remove bond0
100% [#] Removing Bond bond0. Please wait...
bond removed : bond0
```

Create the bond for private interfaces (priveth0 & priveth1). You don’t need to input the mode here, as Veritas Access sets the mode by default.

```
Network>bond priv-create
WARNING: Creating a bond on private interfaces will OFFLINE all services. Verify all private interfaces are connected using a switch.
Do you want to continue (y/n) y
100% [#] Bonding interfaces. Please wait...
Private interfaces bond created, the bondname is: privbond0.
```

Remove the bond settings for the private interface bond.

```
Network> bond priv-remove
WARNING: Removing a bond on private interfaces will OFFLINE all services.
Do you want to continue (y/n) y
100% [#] Removing private interface bond privbond0. Please wait...
Private interfaces bond removed : privbond0
```

Change in MTU during bond creation.
<table>
<thead>
<tr>
<th>Nodename</th>
<th>Device</th>
<th>Status</th>
<th>MTU</th>
<th>Detect</th>
<th>Speed</th>
<th>HWaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>node5_1</td>
<td>pubeth0</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:f3</td>
</tr>
<tr>
<td>node5_1</td>
<td>pubeth1</td>
<td>UP</td>
<td>1000</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:fd</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth0</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:e2</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth1</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:ec</td>
</tr>
</tbody>
</table>

Network> bond create pubeth0,pubeth1 1
100% [#] Bonding interfaces. Please wait...
bond created, the bond name is: bond0

Network> ip link show

<table>
<thead>
<tr>
<th>Nodename</th>
<th>Device</th>
<th>Status</th>
<th>MTU</th>
<th>Detect</th>
<th>Speed</th>
<th>HWaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>node5_1</td>
<td>pubeth0</td>
<td>UP</td>
<td>1000</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:f3</td>
</tr>
<tr>
<td>node5_1</td>
<td>pubeth1</td>
<td>UP</td>
<td>1000</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:fd</td>
</tr>
<tr>
<td>node5_1</td>
<td>bond0</td>
<td>UP</td>
<td>1600</td>
<td></td>
<td></td>
<td>00:0c:29:da:c9:e2</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth0</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:ec</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth1</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:ec</td>
</tr>
</tbody>
</table>

9.2.5 SEE ALSO
dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.3 device

9.3.1 SYNOPSIS

device add devicename
device remove devicename
device rename old_name with new_name nodename
device identify devicename nodename [timeout]
device list nodename
device ipmonitor add devicename ipaddress1[,ipaddress2,...]
device ipmonitor del devicename
device ipmonitor show

9.3.2 DESCRIPTION

The network device command is used to add, remove, rename, identify and list NIC devices from Veritas Access-cluster.

A new NIC device or an existing unused/excluded device can be added to Veritas Accesscluster by using the device add command. The given device must be present on all the nodes of the cluster.

device remove command removes the device from cluster control, and if required it can be unplugged from cluster node. When device is removed, all physical and virtual IPs will be deleted from that NIC device. All physical IPs will be kept in free list and will be available for reuse, virtual IPs will not be available for reuse. One need to re-add virtual IPs in case of reuse. After deleting device from Veritas Accesscluster it will be renamed with eth#, where # is lowest available number for interface index in name ‘eth’. And because of this new name may not be same as old eth# name.

Device names can be changed by using the device rename command. Only device of name prefix ‘eth’ can be renamed. Device with new name should not be present on any node of the cluster. In case of mismatches in names of newly added NICs in cluster, one can rename those devices and then add devices in cluster.

device identify command will start visual indicators on NIC hardware if supported and available. This helps to locate the actual, physical NIC on the node. By default the timeout value is 120 seconds.

device list command will print bus IDs and MAC addresses of all the devices on the given node irrespective of NICs PCI exclusion state.

device ipmonitor add command will add monitoring IP address(es) for public NIC devices. Use all to configure ipmonitor for all public devices. A device is considered to be in working condition if it is able to ping at lease one of the monitoring IP addresses.

device ipmonitor del command will delete the existing configuration of monitoring IP address(es) for a NIC device. Use all to delete ipmonitor for all devices.

device ipmonitor show command will display IP address(es) monitoring information for NIC devices along with the state of the NIC devices.

9.3.3 OPTIONS

  node name  The node on which the operation should takes place.

  devicename  Device on which the operation should takes place.
old_name Present interface name.

new_name Expected new interface name.

timeout Input time in seconds.

9.3.4 EXAMPLES

Display the devices.

<table>
<thead>
<tr>
<th>Device</th>
<th>BusID</th>
<th>MAC Addr</th>
<th>Device Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>priveth0</td>
<td>0000:02:00.0</td>
<td>00:50:56:be:00:9e</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>priveth1</td>
<td>0000:02:01.0</td>
<td>00:50:56:be:00:9f</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth0</td>
<td>0000:02:02.0</td>
<td>00:50:56:be:00:a0</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth1</td>
<td>0000:02:03.0</td>
<td>00:50:56:be:00:a1</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>eth1</td>
<td>0000:02:05.0</td>
<td>00:0c:29:7d:d2:8a</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>eth2</td>
<td>0000:02:06.0</td>
<td>00:0c:29:7d:d2:94</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
</tbody>
</table>

To add a device with the name eth2.

Network> device add eth2

Network> device list cls_01

<table>
<thead>
<tr>
<th>Device</th>
<th>BusID</th>
<th>MAC Addr</th>
<th>Device Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>priveth0</td>
<td>0000:02:00.0</td>
<td>00:50:56:be:00:9e</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>priveth1</td>
<td>0000:02:01.0</td>
<td>00:50:56:be:00:9f</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth0</td>
<td>0000:02:02.0</td>
<td>00:50:56:be:00:a0</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth1</td>
<td>0000:02:03.0</td>
<td>00:50:56:be:00:a1</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>eth1</td>
<td>0000:02:05.0</td>
<td>00:0c:29:7d:d2:8a</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>eth2</td>
<td>0000:02:06.0</td>
<td>00:0c:29:7d:d2:94</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
</tbody>
</table>

To delete a device pubeth2 that is shown in the output of device list.

Network> device remove pubeth2

Network> device list cls_01

<table>
<thead>
<tr>
<th>Device</th>
<th>BusID</th>
<th>MAC Addr</th>
<th>Device Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>priveth0</td>
<td>0000:02:00.0</td>
<td>00:50:56:be:00:9e</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>priveth1</td>
<td>0000:02:01.0</td>
<td>00:50:56:be:00:9f</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth0</td>
<td>0000:02:02.0</td>
<td>00:50:56:be:00:a0</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
<tr>
<td>pubeth1</td>
<td>0000:02:03.0</td>
<td>00:50:56:be:00:a1</td>
<td>82545EM Gigabit Ethernet Controller</td>
</tr>
</tbody>
</table>

9.3. device 117
To identify a device `eth1` on cluster node 1 with a timeout of 60 seconds.

```
Network> device identify eth1 cls_01 60
```

To rename device `eth1` with `eth0` on cluster node 1.

```
Network> device rename eth1 with eth0 cls_01
```

To add a monitoring IP addresses for device `pubeth0`.

```
Network> device ipmonitor add pubeth0 10.29.29.29,10.29.29.30
```

To delete the monitoring IP addresses for all public devices.

```
Network> device ipmonitor del all
```

To show the monitoring IP addresses for all public devices.

```
Network> device ipmonitor show
Device       Monitor IPs   dsga_01   dsga_02
------------- -------- ------ ------
pubeth0      10.209.107.55 ONLINE ONLINE
pubeth1      10.209.107.55 ONLINE ONLINE
```

### 9.3.5 SEE ALSO

`bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), swap(1), pciexclusion(1)`
9.4 dns

9.4.1 SYNOPSIS

dns show
dns enable
dns disable
dns set domainname domainname
dns set nameservers nameserver1 [nameserver2] [nameserver3]
dns set searchdomains searchdomain1 [,searchdomain2] [,searchdomain3]
dns clear domainname
dns clear nameservers

9.4.2 DESCRIPTION

The network dns command is used to view or change the DNS settings.

9.4.3 OPTIONS

- **dns show**: Show the current DNS settings. Show whether DNS is enabled or disabled, and the current values for the domain name and name servers.
- **dns enable**: Enable DNS usage.
- **dns disable**: Disable DNS usage.
- **dns set domainname domainname**: Set the domain name of the server to domainname. To clear the domain name, use `dns clear domainname`.
- **dns set nameservers nameserver1 [nameserver2] [nameserver3]**: Modify the DNS name servers that are used. Specify the name servers in the order in which the name servers should be used. Specify up to three name servers. To clear the name servers list, use `dns clear nameservers`.
- **dns set searchdomains searchdomain1 [,searchdomain2] [,searchdomain3]**: Modify the DNS search domains that are used. Specify the search domains in the order in which the search domains should be used.
- **dns clear domainname**: Clear the domain name used by DNS.
- **dns clear nameservers**: Clear the name servers list used by DNS.

9.4.4 EXAMPLES

Display the current DNS settings.

```
Network> dns show
DNS Status : Enabled
domain : cluster1.com
nameserver : 10.216.50.132
```

Show and then enable the usage of DNS.
Network> dns show
DNS Status : Disabled
Old Settings
----------
domain : cluster1.com
nameserver : 10.216.50.132

Network> dns enable
Network> dns show
DNS Status : Enabled
domain : cluster1.com
nameserver : 10.216.50.132

Disable the usage of DNS.

Network> dns disable
Network> dns show
DNS Status : Disabled
Old Settings
----------
domain : cluster1.com
nameserver : 10.216.50.132

Change the DNS domainname.

Network> dns set domainname example.com
Network> dns show
DNS Status : Enabled
domain : example.com
nameserver : 10.216.50.132

Clear the domain name being used.

Network> dns clear domainname
Network> dns show
DNS Status : Enabled
nameserver : 10.216.50.132

Set the name servers as 10.216.50.199 and 10.216.50.200.

Network> dns set nameservers 10.216.50.199 10.216.50.200
Network> dns show
DNS Status : Enabled
nameserver : 10.216.50.199
nameserver : 10.216.50.200

Remove all name servers that are being used.

Network> dns clear nameservers
Network> dns show
DNS Status : Enabled

9.4.5 SEE ALSO
bond(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.5 firewall

9.5.1 SYNOPSIS

firewall status
firewall enable
firewall disable

9.5.2 DESCRIPTION

The network firewall command is used to view or change the firewall settings.

9.5.3 OPTIONS

   firewall status  Display whether the current firewall status is enabled or disabled.
   firewall enable  Enable the firewall setting to allow specific IPs to connect to the ports while blocking other connections.
   firewall disable Disable the firewall setting and allow connections on any port from any IP. Applied rules do not work when the firewall setting is disabled.

9.5.4 EXAMPLES

Display the current firewall settings.

   Network> firewall status
   Firewall status : DISABLED

Enable firewall.

   Network> firewall enable
   ACCESS net INFO V-288-0 Firewall successfully enabled

Disable firewall.

   Network> firewall disable
   It is not advisable to disable firewall. Do you want you continue (y/n): y
   ACCESS net INFO V-288-0 Firewall successfully disabled

9.5.5 SEE ALSO

bond(1), ip(1), nis(1), nsswitch(1), ping(1), show(1), device(1)
9.6 ip

9.6.1 SYNOPSIS

```sh
ip link set nodename device \{ up | down | mtu MTU \}
ip link show [nodename] \[device\]
ip addr modify oldipaddr newipaddr \{ netmask | prefix \}
ip addr del ipaddr
ip addr add ipaddr \{ netmask | prefix \} type \[device\] \[nodename\]
ip addr online ipaddr nodename
ip addr show
ip route show [nodename]
ip route add nodename ipaddr \{ netmask | prefix \}
               via gateway \[dev device\]
ip route del nodename ipaddr \{ netmask | prefix \}
```

9.6.2 OPTIONS

- **nodename** Node on which the operation takes place. A value of all indicates the operation takes place on all nodes of the cluster.
- **device** Device on which the operation takes place.
- **ipaddr** Specifies the IP address. You can specify either an IPv4 address, or an IPv6 address.
- **oldipaddr** Specifies the old IP address to be modified.
- **newipaddr** Specifies what the new IP address will be.
- **netmask** Netmask for the IPv4 address. Specify an IPv4 address in the format AAA.BBB.CCC.DDD, where each number ranges from 0 to 255.
- **prefix** Prefix length for the IPv6 address. The accepted range is 0-128 integers.
- **up** Changes the state of the device to up.
- **down** Changes the state of the device to down.
- **mtu MTU** The Maximum Transmission Unit (MTU) of the device.
- **type** Specifies how the ipaddr should be used by the cluster. The `type` can be physical or virtual. Physical IP addresses are bound to an interface. Virtual IP addresses can be moved from one interface to other. NFS is served using the virtual IP addresses.

```
ip link set nodename device \{ up | down | mtu MTU \} Change network device attributes or states.
               Use all to change attributes on all nodes. Devices that are part of a bond interface can not be configured through this command. MTU changes to a bond interface get applied to all the interfaces that are part of that bond. Note: Setting the incorrect MTU value will cause the console ip to be unavailable.
ip link show[nodename] \[device\] Display device attributes.
```
**ip addr add** ipaddr netmask|prefix type [device] [nodename] Add a new IP address. IP is a protocol that allows addresses to be attached to a network device. Each device must have at least one address to use the corresponding protocol. Both IPv4 and IPv6 addresses can be attached to one device. The type can be physical or virtual. The device attribute can be used with IP type virtual. If the value type is physical, and the value of device and nodename are valid given physical IP will be added for input device. If no device and nodename configured input physical IP will be added to free list.

**ip addr del** ipaddr Delete an IP address from the cluster. Physical IP addresses can be deleted only if they are not being used by any interface of any node in the cluster, or either type of physical IP is present on interface. Minimum one type of physical IP should be present on interface. Virtual IP addresses, except the console IP address, can be deleted.

**ip addr modify** oldipaddr newipaddr netmask|prefix Modify an IP address used by the cluster. Physical IP addresses and virtual IP addresses can both be modified. Virtual IP address modifications cause NFS connections on oldipaddr to be terminated.

**ip addr online** ipaddr nodename Bring an IP address online for a running node of the cluster.

**ip addr show** Shows the IP addresses being used.

**ip route add** nodename ipaddr netmask|prefix via gateway [dev device] Add a new route for the cluster. The routing table contains information about paths to other networked nodes. Routing table changes can be made per node of the cluster. Use all for nodename to add the route to all nodes of the cluster. Use a netmask(prefix for IPv6) value of 255.255.255.255(128 for IPv6) for the netmask to add a host route to ipaddr. Use a value of 0.0.0.0(: for IPv6) for the gateway to add a route that does not use any gateway. The dev device is an optional argument. Use any of the public devices for the device (pubeth0, pubeth1, or any).

**ip route del** nodename ipaddr netmask|prefix Delete a route used by the cluster. Use all for nodename to delete the route from all nodes of the cluster. The combination of ipaddr and netmask specifies the network or hostg for which the route is deleted. Use a value of 255.255.255.255(128 for IPv6) for the netmask|prefix to delete a host route to ipaddr.

**ip route show [nodename]** Display the routing table of the nodes in the cluster. Use all to see the routing table from all nodes of the cluster.

### 9.6.3 EXAMPLES

Display the current link attributes and states.

```
Network> ip link show

<table>
<thead>
<tr>
<th>Nodename</th>
<th>Device</th>
<th>Status</th>
<th>MTU</th>
<th>Detect</th>
<th>Speed</th>
<th>HWaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>node5_1</td>
<td>pubeth0</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:f3</td>
</tr>
<tr>
<td>node5_1</td>
<td>pubeth1</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:fd</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth0</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:e2</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth1</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:ec</td>
</tr>
</tbody>
</table>
```

View the attributes and state of a specific node and a specific interface.

```
Network> ip link show node5_2 pubeth0

<table>
<thead>
<tr>
<th>Nodename</th>
<th>Device</th>
<th>Status</th>
<th>MTU</th>
<th>Detect</th>
<th>Speed</th>
<th>HWaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>node5_2</td>
<td>pubeth0</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:f3</td>
</tr>
</tbody>
</table>
```

Set the MTU value on all nodes for a specific device.

9.6. ip 123
Network> ip link set all pubeth0 mtu 1600
Network> ip link show
<table>
<thead>
<tr>
<th>Nodename</th>
<th>Device</th>
<th>Status</th>
<th>MTU</th>
<th>Detect</th>
<th>Speed</th>
<th>HWaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>node5_1</td>
<td>pubeth0</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:f3</td>
</tr>
<tr>
<td>node5_1</td>
<td>pubeth1</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:a8:9d:fd</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth0</td>
<td>UP</td>
<td>1600</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:e2</td>
</tr>
<tr>
<td>node5_2</td>
<td>pubeth1</td>
<td>UP</td>
<td>1500</td>
<td>yes</td>
<td>100Mb/s</td>
<td>00:0c:29:da:c9:ec</td>
</tr>
</tbody>
</table>

Display the IP addresses used by the cluster and their states.

Network> ip addr show
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.217</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

Add an IP address to the physical IP addresses used by the cluster.

Network> ip addr add 10.216.114.216 255.255.248.0 physical
Network> ip addr show
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.216</td>
<td>255.255.248.0</td>
<td>( unused )</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

Add an IP address to the virtual IP addresses used by the cluster.

Network> ip addr add 10.10.10.14 255.255.248.0 virtual
Network> ip addr show
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.216</td>
<td>255.255.248.0</td>
<td>( unused )</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.14</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
Add an IP address to the virtual IP addresses used by the cluster for a VLAN device

```
Network> ip addr add 10.10.10.14 255.255.248.0 virtual pubeth1.2
Network> ip addr show
```

```
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.216</td>
<td>255.255.248.0</td>
<td>pubeth1.2</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.217</td>
<td>255.255.248.0</td>
<td>pubeth0.2</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.218</td>
<td>255.255.248.0</td>
<td>( unused )</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.219</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.14</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
```

Delete an IP address from the physical IP addresses being used by the cluster. Physical IP addresses that are assigned to a device cannot be deleted; they can only be modified. The virtual IP address for the console cannot be deleted; it can only be modified.

```
Network> ip addr del 10.216.114.216
Network> ip addr show
```

```
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.216</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.14</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
```

Modify an IP address from the IP addresses being used by the cluster. Physical IP addresses which are assigned to a device cannot be deleted; they can only be modified. The virtual IP address for the console cannot be deleted; it can only be modified.

```
Network> ip addr modify 10.10.10.14 10.10.10.15 255.255.248.0
Network> ip addr show
```

```
<table>
<thead>
<tr>
<th>IP</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.217</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.10.10.10</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.11</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.12</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.13</td>
<td>255.255.248.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.10.10.14</td>
<td>255.255.248.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
```
Online an IP protocol address used by the cluster on any running node of the cluster.

```
Network> ip addr online 10.10.10.15 node5_2
Network> ip addr show
```

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Netmask</th>
<th>Device</th>
<th>Node</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.216.114.212</td>
<td>255.255.255.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.213</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>node5_1</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.214</td>
<td>255.255.255.0</td>
<td>pubeth0</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.215</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Physical</td>
<td></td>
</tr>
<tr>
<td>10.216.114.216</td>
<td>255.255.255.0</td>
<td>pubeth0</td>
<td>node5_1</td>
<td>Virtual</td>
<td>ONLINE (Con IP)</td>
</tr>
<tr>
<td>10.216.114.217</td>
<td>255.255.255.0</td>
<td>pubeth1</td>
<td>node5_2</td>
<td>Virtual</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>

View the routing table of a specific node in the cluster.

```
Network> ip route show node5_2
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>Irtt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.89.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>priveth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth1</td>
</tr>
<tr>
<td>10.254.0.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>10.216.112.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
</tbody>
</table>

Add a route through a given device to the routing table of all nodes in the cluster. Use a value of 0.0.0.0 for the gateway, to use a route that is based on only the device and does not use any gateway.

```
Network> ip route add all 10.216.128.0 255.255.248.0 via 0.0.0.0
Network> ip route show
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>Irtt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.89.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>priveth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth1</td>
</tr>
<tr>
<td>10.254.0.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>10.216.112.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
</tbody>
</table>

Delete the default gateway being used by a specific node. The deletion only aim at static routes which are added by command(ip route add).
Network> ip route del node5_2 10.216.128.0 255.255.248.0 via 0.0.0.0
Network> ip route show node5_2
node5_2

<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS</th>
<th>Window</th>
<th>irtt</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.89.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>priveth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.248.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.248.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth1</td>
</tr>
<tr>
<td>10.254.0.0</td>
<td>0.0.0.0</td>
<td>255.255.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
</tbody>
</table>

9.6.4 SEE ALSO

bond(1), dns(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.7 krb

9.7.1 SYNOPSIS

```
krb standalone set kdc_server kerberos_realm keytab_file
krb standalone unset
krb standalone show
```

9.7.2 OPTIONS

- **kdc_server**  Kerberos KDC server.
- **kerberos_realm**  Kerberos realm.
- **keytab_file**  Location of keytab file on the console node.

```
krb standalone set kdc_server kerberos_realm keytab_file
```

This command enables Kerberos authentication for NFS mounts. This would set Kerberos configuration on Veritas Access given the KDC server, Kerberos realm and the keytab file. Keytab file should have been uploaded to the Veritas Access console node. Keytab file will be copied from the console node to /etc/krb5.keytab on all of the nodes of the cluster. Kerberos will be configured on all of the nodes of the cluster. Keytab file should have been set up with clustername as the hostname. Kerberos cannot be configured with standalone KDC if CIFS is already configured with ads. This command also checks for the correct domain in the `/etc/idmapd.conf` file. If the domain is not set, NFSv4 idmapping will not be proper and the command will throw a warning to set the domain.

- **krb standalone show**  Display the Kerberos configuration.
- **krb standalone unset**  Reset the Kerberos configuration.

9.7.3 EXAMPLES

```
test_fa.Network> krb standalone set kdc_server TESTKDC.COM /home/support/krb5.keytab
ACCESS krb SUCCESS V-288-999 Kerberos configured for NFS

test_fa.Network> krb standalone show
Kerberos General Info:
======================
KDC: kdc_server
REALM: TESTKDC.COM

Keytab Info:
------------
Keytab name: FILE:/etc/krb5.keytab

<table>
<thead>
<tr>
<th>KVNO</th>
<th>Timestamp</th>
<th>Principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>07/07/15 16:02:54</td>
<td>nfs/test_fa@TESTKDC.COM (aes256-cts-hmac-shal-96)</td>
</tr>
<tr>
<td>2</td>
<td>07/07/15 16:02:54</td>
<td>nfs/test_fa@TESTKDC.COM (aes128-cts-hmac-shal-96)</td>
</tr>
<tr>
<td>2</td>
<td>07/07/15 16:02:54</td>
<td>nfs/test_fa@TESTKDC.COM (des3-cbc-shal)</td>
</tr>
<tr>
<td>2</td>
<td>07/07/15 16:02:54</td>
<td>nfs/test_fa@TESTKDC.COM (arcfour-hmac)</td>
</tr>
<tr>
<td>2</td>
<td>07/07/15 16:02:54</td>
<td>nfs/test_fa@TESTKDC.COM (des-hmac-shal)</td>
</tr>
<tr>
<td>2</td>
<td>07/07/15 16:02:55</td>
<td>nfs/test_fa@TESTKDC.COM (des-cbc-md5)</td>
</tr>
</tbody>
</table>

test_fa.Network> krb standalone unset
```
<table>
<thead>
<tr>
<th>ACCESS krb SUCCESS V-288-999 Kerberos configuration is reset</th>
</tr>
</thead>
<tbody>
<tr>
<td>test_fa.Network&gt; krb standalone show</td>
</tr>
<tr>
<td>Kerberos is not configured</td>
</tr>
<tr>
<td>test_fa.Network&gt;</td>
</tr>
</tbody>
</table>
## 9.8 ldap

### 9.8.1 SYNOPSIS

ldap enable
ldap disable
ldap show [users|groups|netgroups]
ldap set { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash } value
ldap get { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash }
ldap clear { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash }

### 9.8.2 DESCRIPTION

The network ldap commands are used to configure the Lightweight Directory Access Protocol (LDAP) client for authentication. These commands configure the system to use LDAP users and groups when logging into the system. LDAP clients use the LDAPv3 protocol for communicating with the server. Enabling the LDAP client configures the Pluggable Authentication Module (PAM) for LDAP users and groups. PAM is the standard authentication framework for Linux.

### 9.8.3 OPTIONS

- **value** Value of the variable to set.
- **ldap enable** Enable the LDAP client, and configure PAM configuration files to use LDAP.
- **ldap disable** Disable the LDAP client, and configure PAM configuration files not to use LDAP.
- **ldap show** Display the LDAP client configuration.
- **ldap show users** Display the LDAP users that are available in the NSS database.
- **ldap show groups** Display the LDAP groups that are available in the NSS database.
- **ldap show netgroups** Display the LDAP netgroups that are available in the NSS database.
- **ldap set server** value Set the LDAP server’s host name or IP address. This setting is mandatory.
- **ldap set port** value Set the LDAP server’s port. Default value is 389.
- **ldap set basedn** value Set the LDAP base Distinguished Name (DN). This setting is mandatory.
- **ldap set ssl** { on|off } Set LDAP over Secure Sockets Layer (SSL) to be on or off. Set this option to “on” if your LDAP server supports SSL. Certificates required for SSL are auto-negotiated with the LDAP server during session establishment. The default value is “off.” This setting is mandatory.
- **ldap set binddn** value Set the LDAP bind DN and its password. This DN is used to bind with the LDAP server for “read” access. For authentication, “read” access to most of the attributes is required. This setting is mandatory.
**ldap set rootbinddn value**  Set the LDAP root bind DN and its password. This DN is used to bind with the LDAP server for “write” access. This setting is not required for authentication. To change some attributes of an LDAP entry, this DN is required. For example, changing a user’s password by root (uid=0) user requires admin privileges to write into the LDAP directory. This setting is optional.

**ldap set users-basedn value**  Set the LDAP users base DN. This DN is used by the authentication system (PAM and NSS) to search LDAP users. This setting is mandatory.

**ldap set groups-basedn value**  Set the LDAP groups base DN. This DN is used by the authentication system (PAM and NSS) to search the LDAP groups. This setting is mandatory.

**ldap set netgroups-basedn value**  Set the LDAP netgroups base DN. This DN is used by the authentication system (PAM and NSS) to search the LDAP netgroups. This setting is mandatory.

**ldap set password-hash { clear|crypt|md5 }**  Set the password hash to use when setting an LDAP user’s password. The password will be encrypted with the configured hash algorithm before sending it to the LDAP server for storing into the LDAP directory. This setting is optional.

**ldap get { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash }**  Get the values of the configured settings.

**ldap clear { server|port|basedn|binddn|ssl|rootbinddn|users-basedn|groups-basedn|netgroups-basedn|password-hash }**  Clears a specified attribute and sets to default.

### 9.8.4 EXAMPLES

Enable the LDAP client.

```
Network> ldap enable
```

Disable the LDAP client.

```
Network> ldap disable
```

Display the LDAP client configuration.

```
Network> ldap show
LDAP client is enabled.
==================================
LDAP server:  ldap_server
LDAP port:  389 (default)
LDAP base DN:  dc=example,dc=com
LDAP over SSL:  on
LDAP bind DN:  cn=binduser,dc=example,dc=com
LDAP root bind DN:  cn=admin,dc=example,dc=com
LDAP password hash:  md5
LDAP users base DN:  ou=Users,dc=example,dc=com
LDAP groups base DN:  ou=Groups,dc=example,dc=com
LDAP netgroups base DN:  ou=Netgroups,dc=example,dc=com
OK Completed
```

Display the LDAP users available to the authentication system.

```
Network> ldap show users
==========================
User 'ldapuser1':
==========================
Username:  Username Surname
```
uid: 2000
gid: 2000
Home Directory: /home/ldapuser1
Login Shell: /bin/bash

Display the LDAP groups available to the authentication system.

```
Network> ldap show groups
=============
Group '2000':
=============
Groupname: group1
Members of the Group: ldapuser1
```

Show LDAP netgroups available to the authentication system.

```
Network> ldap show netgroups
Using ldap-server.example.com as LDAP server and 389 as LDAP port.
=============
Netgroup 'netgroup1':
=============
<table>
<thead>
<tr>
<th>Host</th>
<th>User</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>host1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>host2</td>
<td>admin</td>
<td>-</td>
</tr>
</tbody>
</table>

=============
Netgroup 'netgroup2':
=============
<table>
<thead>
<tr>
<th>Host</th>
<th>User</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>host3</td>
<td>testadmin</td>
<td>-</td>
</tr>
</tbody>
</table>
```

Configure the LDAP server name.

```
Network> ldap set server ldap-server.example.com
OK Completed
```

Get the configured LDAP server name.

```
Network> ldap get server
LDAP server: ldap-server.example.com
OK Completed
```

Configure the LDAP server port.

```
Network> ldap set port 555
OK Completed
```

Get the configured LDAP server port.

```
Network> ldap get port
LDAP port: 555
OK Completed
```

Configure the base DN.

```
Network> ldap set basedn dc=example,dc=com
OK Completed
```
Get the configured base DN.

```
Network> ldap get basedn
LDAP base DN: dc=example,dc=com
OK Completed
```

Configure LDAP over SSL to on.

```
Network> ldap set ssl on
OK Completed
```

Get LDAP over SSL setting.

```
Network> ldap get ssl
LDAP over SSL: on
OK Completed
```

Configure the bind DN.

```
Network> ldap set binddn cn=binduser,dc=example,dc=com
Enter password for 'cn=binduser,dc=example,dc=com': ********
OK Completed
```

Get the configured bind DN.

```
Network> ldap get binddn
LDAP bind DN: cn=binduser,dc=example,dc=com
OK Completed
```

Configure the root bind DN.

```
Network> ldap set rootbinddn cn=rootuser,dc=example,dc=com
Enter password for 'cn=rootuser,dc=example,dc=com': ********
OK Completed
```

Get the configured root bind DN.

```
Network> ldap get binddn
LDAP root bind DN: cn=rootuser,dc=example,dc=com
OK Completed
```

Configure the password hash.

```
Network> ldap set password-hash clear
OK Completed
```

Get the configured password hash.

```
Network> ldap get password-hash
LDAP password hash: clear
OK Completed
```

Configure the users base DN.

```
Network> ldap set users-basedn ou=Users,dc=example,dc=com
OK Completed
```

Get the configured users base DN.

9.8. ldap
Configure the groups base DN.

 Network> ldap set groups-basedn ou=Groups,dc=example,dc=com
 OK Completed

Get the configured groups base DN.

 Network> ldap get groups-basedn
 LDAP groups base DN: ou=Groups,dc=example,dc=com
 OK Completed

Configure the netgroups base DN.

 Network> ldap set netgroups-basedn ou=Netgroups,dc=example,dc=com
 OK Completed

Get the configured netgroups base DN.

 Network> ldap get netgroups-basedn
 LDAP netgroups base DN: ou=Netgroups,dc=example,dc=com
 OK Completed

Clear a specified attribute.

 Network> ldap clear <attribute>
 OK Completed

9.8.5 SEE ALSO

bond(1), dns(1), ip(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.9 loadbalance

9.9.1 SYNOPSIS

loadbalance configure [vip]
loadbalance remove

9.9.2 DESCRIPTION

The network loadbalance command configures a single VIP to act as a load balancer which distributes the incoming request to the cluster. The command can also remove the load balance configuration.

9.9.3 OPTIONS

    loadbalance configure VIP  Configure the loadbalancer for given VIP.
    loadbalance remove        Remove the loadbalance configuration.

9.9.4 EXAMPLES

To configure the loadbalancer.

Network> loadbalance configure 10.216.114.216
Loadbalancer configured successfully on VIP 10.216.114.216 using node clusternode_01 as router

To remove the loadbalance configuration.

Network> loadbalance remove

9.9.5 SEE ALSO

ipvsadm(1)
9.10 netgroup

9.10.1 SYNOPSIS

netgroup add groupname memberlist
netgroup delete groupname [memberlist]
netgroup show [groupname]

9.10.2 DESCRIPTION

The netgroup commands are used to view, add, or delete local netgroups.

The netgroup file defines “netgroups”, which are sets of (host, user, domain) tuples, used for permission checking when doing remote mounts, remote logins and remote shells. Each line in the file consists of a netgroup name followed by a list of members, where a member is either another netgroup name, or a triple:

(hos,t,user,domain)

where the host, user, and domain are character strings for the corresponding components. Any of the three fields can be empty, in which case specifies a “wildcard”, or the string “-” to specify “no valid value”. The domain field must either be the local domain name or empty for the netgroup entry to be used. This field does not limit the netgroup or provide security. The domain field refers to the domain in which the triple is valid, not the domain containing the the trusted host.

When exporting a directory by NFS with the specified options, clients may be specified in netgroups. Netgroups may be identified using @group. Only the host part of each netgroup member is considered when checking for membership:

NFS> share add rw,async /vx/fs1/share @client_group

Note, the netgroup takes effect only after adding “files” to the netgroup of Name Service Switch (NSS) configuration:

Network> nsswitch conf group files nis

When adding data to any existing netgroup, the new data cannot be the same as the existing data of that netgroup. If you are adding data to a non-existent netgroup, you need to create a new netgroup. You can delete the data of an existing netgroup. If you delete a netgroup without a member list, you delete the netgroup.

9.10.3 OPTIONS

    groupname  netgroup name.
    memberlist  comma-separated member list. A member can be an IPv4 address, IPv6 address, netgroup name, or a hostname. The hostname can include the characters: a-zl A-Zl0-9 or a hyphen (-). Each level of the hostname should between 1 and 63 characters long and should not start or end with a hyphen (-). The last TLD (Top Level Domain) must be at least two characters and a maximum of six characters. If the member is not a netgroup name, it will be filled in as the host.

    netgroup add groupname memberlist  Add members to an existing netgroup or create a new netgroup.

    netgroup delete groupname [memberlist]  Delete the members of an existing netgroup or delete netgroup.

    netgroup show [groupname]  Display the netgroup settings.
9.10.4 EXAMPLES

To create a netgroup with members another netgroup name, IPv4 address, IPv6 address, and hostname

```
Network> netgroup add test_group2 vip,10.200.114.173,cdc.testhost.com,2002:4559:1fe2:0:0:0:45:88
```

```
Network> netgroup show
Name Member List
------------- -----------
test_group1 192.168.0.8,cdc.myhost.com,2002:4559:1fe2:0:0:0:4559:1f
```

```
Network> netgroup add test_group1 10.200.114.250
```

```
Network> netgroup show
Name Member List
------------- -----------
test_group1 10.200.114.250,192.168.0.8,cdc.myhost.com,2002:4559:1fe2:0:0:0:4559:1f
```

```
Network> netgroup delete test_group2 2002:4559:1fe2:0:0:0:45:88,cdc.testhost.com,vip
```

```
Network> netgroup show
Name Member List
------------- -----------
test_group1 10.200.114.250,192.168.0.8,cdc.myhost.com,2002:4559:1fe2:0:0:0:4559:1f
```

To delete an existing netgroup

```
Network> netgroup delete test_group2
```

```
Network> netgroup show
Name Member List
------------- -----------
test_group1 10.200.114.250,192.168.0.8,cdc.myhost.com,2002:4559:1fe2:0:0:0:4559:1f
```

Display the netgroup.

```
Network> netgroup show test_group1
Name Member List
------------- -----------
test_group1 192.168.0.8,cdc.myhost.com,2002:4559:1fe2:0:0:0:4559:1f
```

9.10.5 SEE ALSO

bond(1), dns(1), ip(1), ldap(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.11 nis

9.11.1 SYNOPSIS

nis show [users|groups|netgroups]
nis disable
nis enable
nis set servername servername
nis set domainname [domainname]

9.11.2 DESCRIPTION

The network nis commands set or display the domain name on all of the nodes. The commands can also enable or disable NIS clients on all of the nodes.

9.11.3 OPTIONS

- nis show Display the NIS server name and domain name.
- nis show users Show NIS users that are available in the NIS database.
- nis show groups Show NIS groups that are available in the NIS database.
- nis show netgroups Show NIS netgroups that are available in the NIS database.
- nis disable Disable the NIS clients on all the nodes.
- nis enable Enable NIS clients on all the nodes.
- nis set servername servername Set the NIS server name on all the nodes.
- nis set domainname [domainname] Set the NIS domain name on all the nodes.

9.11.4 EXAMPLES

To display the current status of NIS.

```
Network> nis show
NIS Status : Disabled
domain :
NIS Server :
```

To display NIS netgroups that are available in the NIS database.

```
Network> nis show netgroups
NetGroupname : netgrp3
Members of the Group : (testqa-13.testqa.com,,-)
NetGroupname : netgrp2
```

To display NIS groups that are available in the NIS database.
Network> nis show groups
  Groupname : webservd
  Members of the Group :
  Groupname : sysadmin
  Members of the Group :
  Groupname : noaccess
  Members of the Group :

To display NIS users that are available in the NIS database.

Network> nis show users
  User : root
  Name : Super-User
  uid : 0
  gid : 0
  Home Directory : /
  Login Shell : /sbin/sh

  User : u2
  Name :
  uid : 101
  gid : 1
  Home Directory : /lhome/u2
  Login Shell : /bin/sh

To set the domain name.

Network> nis set domainname vxindia.veritas.com
  Setting domainname: "vxindia.veritas.com"

To set the server name.

Network> nis set servername vmlxpxl.vxindia.veritas.com
  Setting NIS Server "vmlxpxl.vxindia.veritas.com"

To enable NIS.

Network> nis enable

To check whether NIS is enabled or not, run the following command:

Network> nis show
  NIS Status : Enabled
  domain : vxindia.veritas.com
  NIS Server : vmlxpxl.vxindia.veritas.com

To disable the NIS.

Network> nis disable

9.11.5 SEE ALSO

bond(1), dns(1), ip(1), ldap(1), netgroup(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.12 nsswitch

9.12.1 SYNOPSIS

nsswitch show
nsswitch conf { group|hosts|netgroup|passwd|shadow } value1 value2 value3 value4

9.12.2 DESCRIPTION

The network nsswitch commands display or change the Name Service Switch (NSS) configuration.

9.12.3 OPTIONS

nsswitch show  Display the name service switch configuration.

nsswitch conf { group|hosts|netgroup|passwd|shadow } value1 value2 value3 value4
Configure the method for the name service switch lookup process. Specify the name service switch lookup order with the following values:

value1: Choose the type {files} {files}
value2: Enter one of the following types { files | nis | winbind | ldap }
value3: Enter one of the following types { files | nis | winbind | ldap }
value4: Enter one of the following types { files | nis | winbind | ldap }

To configure nsswitch conf host value1 value2 value3 enter the following:
value1: Choose the type {files} {files}
value2: Enter one of the following types { files | nis | dns }
value3: Enter one of the following types { files | nis | dns }

To configure nsswitch conf netgroup value1 value2 value3, enter the following:
value1: Enter one of the following types { files | nis | winbind | ldap }
value2: Enter one of the following types { files | nis | winbind | ldap }

9.12.4 EXAMPLES

To display the current value set on nsswitch for all group, hosts, netgroup, passwd and shadow

```
Network> nsswitch show
group: files nis winbind ldap
hosts: files nis dns
netgroup: files nis
passwd: files nis winbind ldap
shadow: files nis winbind
```

Change the order of the group items.

```
Network> nsswitch conf group nis files
```

Immediate effect of above command can be seen by using the show command.
Network> nsswitch show
group: files nis
hosts: files nis dns
netgroup: nis files
passwd: files nis winbind ldap
shadow: files nis winbind

To configure netgroup
Network> nsswitch conf netgroup files ldap nis

To configure passwd
Network> nsswitch conf passwd files winbind ldap nis

To configure shadow
Network> nsswitch conf shadow files winbind

9.12.5 SEE ALSO
bond(1), dns(1), ip(1), nis(1), ldap(1), netgroup(1), ping(1), show(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.13 pciexclusion

9.13.1 SYNOPSIS

pciexclusion show
pciexclusion add pcilist
pciexclusion delete pci

9.13.2 OPTIONS

**pcilist** This includes comma-separated list of PCI IDs. The PCI ID bits format is hexadecimal. (XXXX:XX:XX.X).

**pci** The PCI ID bits format is hexadecimal (XXXX:XX:XX.X).

**pciexclusion show** Displays the PCI IDs that have been selected for exclusion. It also provides information about whether it has been excluded or not by displaying y(yes) or n(no) symbols corresponding to the node name. If the node is in the INSTALLED state, it displays the UUID of the node.

**pciexclusion add pcilist** Allows an administrator to add specific PCI ID(s) for exclusion. These values must be provided before doing the installation. It then excludes the PCI from the second node installation.

**pciexclusion delete pci** Allows an administrator to delete a given PCI ID from exclusion. This command must be used before doing the installation for it to take effect.

9.13.3 EXAMPLES

Display the PCI IDs.

<table>
<thead>
<tr>
<th>PCI ID</th>
<th>EXCLUDED</th>
<th>NODENAME/UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>test_1</td>
</tr>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>a79a7f43-9fe2-4eeb-aalf-27a70e7a0820</td>
</tr>
<tr>
<td>0000:04:00:1</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

Add the PCI ID for exclusion.

<table>
<thead>
<tr>
<th>PCI ID</th>
<th>EXCLUDED</th>
<th>NODENAME/UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>test_1</td>
</tr>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>a79a7f43-9fe2-4eeb-aalf-27a70e7a0820</td>
</tr>
<tr>
<td>0000:04:00:1</td>
<td>n</td>
<td></td>
</tr>
<tr>
<td>0000:00:09.0</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

Delete the PCI ID from exclusion.
Support> pciexclusion delete 0000:04:00:1
Support> pciexclusion show

<table>
<thead>
<tr>
<th>PCI ID</th>
<th>EXCLUDED</th>
<th>NODENAME/UUID</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>test_1</td>
</tr>
<tr>
<td>0000:0e:00.0</td>
<td>y</td>
<td>a79a7f43-9fe2-4eeb-a1f-27a70e7a0820</td>
</tr>
<tr>
<td>0000:00:09.0</td>
<td>n</td>
<td></td>
</tr>
</tbody>
</table>

9.13.4 SEE ALSO

bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1)
9.14 ping

9.14.1 SYNOPSIS

ping destination [nodename] [devicename] [packets]

9.14.2 DESCRIPTION

The network ping command is used to test whether a particular host or gateway is reachable across an IP network.

9.14.3 OPTIONS

- **destination** The host or gateway to send the information to. The destination field can contain either a DNS name or an IP address.
- **nodename** Node from which the ping takes place. A value of any indicates the ping can be done from any node in the cluster.
- **devicename** Device through which the ping takes place. A value of any indicates the ping can be done from any device in the cluster.
- **packets** Number of packets to be sent to the destination. The default is 5.

9.14.4 EXAMPLES

Test whether destination is reachable across an IP network.

```
Network> ping somenode
PING somenode.domain.com (10.216.2.11) 56(84) bytes of data.
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=3 ttl=64 time=0.167 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=4 ttl=64 time=0.114 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=5 ttl=64 time=0.160 ms

--- somenode.domain.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.114/0.145/0.167/0.024 ms
```

Test whether destination is reachable across an IP network from nodename.

```
Network> ping somenode node1_1
PING somenode.domain.com (10.216.2.11) 56(84) bytes of data.
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=3 ttl=64 time=0.167 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=4 ttl=64 time=0.114 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=5 ttl=64 time=0.160 ms

--- somenode.domain.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.114/0.145/0.167/0.024 ms
```
Test whether destination is reachable across an IP network from nodename, via a specific devicename.

```
Network> ping somenode node1_1 pubeth0
PING somenode.domain.com (10.216.2.11) 56(84) bytes of data.
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
--- somenode.domain.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.018/0.026/0.057/0.016 ms
```

Test whether destination is reachable across an IP network from nodename, by sending a specified number of packets.

```
Network> ping somenode node1_1 any 2
PING somenode.domain.com (10.216.2.11) 56(84) bytes of data.
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=1 ttl=64 time=0.134 ms
64 bytes from somenode.domain.com (10.216.2.11): icmp_seq=2 ttl=64 time=0.154 ms
--- somenode.domain.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.114/0.145/0.167/0.024 ms
```

9.14.5 SEE ALSO

bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), swap(1), pci exclusion(1)
9.15 show

9.15.1 SYNOPSIS

show

9.15.2 DESCRIPTION

The network show command displays the network configuration and statistics on all of the available nodes.

9.15.3 EXAMPLES

Show the network configuration and statistics.

```
Network> show
Interface Statistics
-------------
node5_1
-----------
<table>
<thead>
<tr>
<th>Interfaces</th>
<th>MTU</th>
<th>Metric</th>
<th>RX-OK</th>
<th>RX-DROP</th>
<th>RX-ERR</th>
<th>RX-FRAME</th>
<th>TX-OK</th>
<th>TX-DROP</th>
</tr>
</thead>
<tbody>
<tr>
<td>pubeth0</td>
<td>1500</td>
<td>0</td>
<td>1484835</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>890443</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>pubeth1</td>
<td>1500</td>
<td>0</td>
<td>1488524</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>890731</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

node5_2 down or cannot connect

Routing Table
-------------
node5_1
-----------
<table>
<thead>
<tr>
<th>Destination</th>
<th>Gateway</th>
<th>Genmask</th>
<th>Flags</th>
<th>MSS Window</th>
<th>mtu</th>
<th>Iface</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.16.1.0</td>
<td>0.0.0.0</td>
<td>255.255.255.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>priveth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.248.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>pubeth0</td>
</tr>
<tr>
<td>10.216.112.0</td>
<td>0.0.0.0</td>
<td>255.255.248.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>pubeth1</td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>0.0.0.0</td>
<td>255.0.0.0</td>
<td>U</td>
<td>0</td>
<td>0</td>
<td>lo</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>10.216.112.1</td>
<td>0.0.0.0</td>
<td>UG</td>
<td>0</td>
<td>0</td>
<td>pubeth1</td>
</tr>
</tbody>
</table>

node5_2 down or cannot connect
```

9.15.4 OUTPUT

**Interface Statistics**

- **Interfaces** The name of the interface.
- **MTU** The Maximum Transmission Unit of the interface.
- **Metric** The routing metric of the interface.
- **RX-OK** Number of received packets.
RX-DROP Number of dropped packets.
RX-ERR Number of error packets.
RX-FRAME Number of packets fails to end on byte boundary.
TX-OK Number of transmitted packets.
TX-DROP Number of dropped packets.
TX-ERR Number of error packets.
TX-CAR Number of carrier lost.

**Flag**

B: BROADCAST L: LOOPBACK M: MULTICAST R: RUNNING U: UP

**Routing Table**

Destination The destination network or destination host.
Gateway The gateway address or ‘*’ if none set.
Genmask The netmask for the destination net; ‘255.255.255.255’ for a host destination and ‘0.0.0.0’ for the default route.
Flags U (route is up) H (target is a host) G (use gateway) R (reinstate route for dynamic routing) D (dynamically installed by daemon or redirect) M (modified from routing daemon or redirect) A (installed by addrconf) C (cache entry) ! (reject route)
Next Hop The the nexthop router of a multipath route.
Metric The ‘distance’ to the target, usually counted in hops.
Ref Number of references to this route.
Use Count of lookups for the route.
MSS Default maximum segment size for TCP connections over this route.
Window Default window size for TCP connections over this route.
irtt Initial RTT (Round Trip Time).
Iface Interface to which packets for this route will be sent.

**9.15.5 SEE ALSO**

bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), vlan(1), device(1), swap(1), pciexclusion(1)
9.16 swap

9.16.1 SYNOPSIS

\texttt{swap \underline{interface1} \underline{interface2} [nodename]}

9.16.2 DESCRIPTION

The system \texttt{swap} command can be used for swapping two network interfaces of a node in a cluster. The System Administrator can use this command with a multi-node cluster only to swap public interfaces. On single node cluster, this command can be used to swap public as well as private interfaces. If input to the \texttt{swap} command contains one public and one private interface, and there are two separate switches for the private and the public network, then before running this command, the System Administrator has to exchange cable connections between these interfaces. This command requires stopping the given interfaces, and after running the \texttt{swap} command, all SSH connection(s) hosted on the input interfaces will terminate. The \texttt{swap} command helps set up the cluster properly in cases where the installation of the first node gateway cannot be pinged and is not to be used with a full-fledged system. It is not recommended that you use this command when you have some CIFS/NFS shares exported. You can check the status of the \texttt{swap} command under \texttt{history}.

9.16.3 OPTIONS

\texttt{\texttt{swap \underline{interface1} \underline{interface2} nodename}  Swap two network interfaces, interface1 and interface2.}

\texttt{interface1} : name of first interface.

\texttt{interface2} : name of second interface.

\texttt{nodename} : name of node. If nodename is not provided, it is executed on the current node.

9.16.4 EXAMPLES

Swap two interfaces.

```
Network> swap pubeth0 priveth0 test_01
All ssh connection(s) to swapped interfaces need to start again after this command.
Do you want to continue [Enter "y/yes" to continue]...
```

Check status of this command in history.

9.16.5 SEE ALSO

\texttt{bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), vlan(1), device(1), pciexclusion(1)
9.17 vlan

9.17.1 SYNOPSIS

vlan show  
vlan add device vlan_id  
vlan del vlan_device

9.17.2 DESCRIPTION

The network vlan command is used to view, add, or delete VLAN interfaces.

By default ip addr add will not use VLAN devices unless explicitly specified in the device attribute. By default, CIFS shares created using share add will not use virtual IPs based on VLAN devices, unless explicitly specified with ip= in share options.

When a VLAN device is deleted, physical IPs that are used by that VLAN device will automatically be freed, and can be seen in the output of ip addr show as unused. When a VLAN device is deleted, virtual IPs configured on that VLAN device will automatically be deleted and will no longer be visible in ip addr show.

9.17.3 OPTIONS

device Device on which VLAN devices needs to be added.

vlan_id VLAN id which the new VLAN device should use. Valid values range from 1-4095.

vlan_device A VLAN device name is a combination of actual device on which the VLAN is based and the VLAN id separated by ‘.’.

vlan show Show the current VLAN devices.

vlan add device vlan_id Add a VLAN device on device with VLAN id as f1vlan_id.

vlan del vlan_device Delete the VLAN device named vlan_device.

9.17.4 EXAMPLES

Display the VLAN devices.

```
Network> vlan show
VLAN DEVICE VLAN id
---- ------ -------
pubeth0.2 pubeth0 2
```

To add a VLAN device with id 2 on pubeth1

```
Network> vlan add pubeth1 2
Network> vlan show
VLAN DEVICE VLAN id
---- ------ -------
pubeth0.2 pubeth0 2
pubeth1.2 pubeth1 2
```
To delete a VLAN device that is shown in the output of `vlan show`

```
Network> vlan del pubeth0.2

Network> vlan show
VLAN     DEVICE      VLAN id
----     ------      ------
pubeth1.2 pubeth1     2
```

### 9.17.5 SEE ALSO

`bond(1), dns(1), ip(1), ldap(1), netgroup(1), nis(1), nsswitch(1), ping(1), show(1), device(1), swap(1), pciexclusion(1)`
10.1 nfs

10.1.1 SYNOPSIS

server [start|stop|status|switch]
stat show [nodename]
stat reset [nodename]
share add nfsoptions export_dir [client]
share delete export_dir [client]
share show
show fs

10.1.2 DESCRIPTION

The nfs commands maintain the current table of exported file systems for the Network File System (NFS).

10.1.3 OPTIONS

nfsoptions Comma-separated list of export options from the set {ro, rw, sync, async, secure, insecure, secure_locks, insecure_locks, root_squash, no_root_squash, wdelay, no_wdelay, subtree_check, no_subtree_check, nordirplus, fsid=<number>, sec=krb5:krb5i:krb5p:sys:none}. For example: ro,root_squash; rw,secure,no_root_squash. The default export options are {ro, sync, secure, secure_locks, root_squash, wdelay, no_subtree_check}. The “no_wdelay” option has no effect if “async” is also set. fsid could be any number between 1 and 1073741823 and it must be unique among all exported paths.

wdelay: For backwards-compatibility, the wdelay and no_wdelay options are still supported, but the options are being deprecated. no_wdelay is the only effective behavior regardless of setting wdelay or no_wdelay option. Clients can handle flushing of data using server COMMIT operations and UNSTABLE writes.

For NFS Ganesha exports, export options {secure_locks, insecure_locks, wdelay, no_wdelay, subtree_check, no_subtree_check, fsid=number} are not supported and will be ignored.
export_dir  Path of the directory that needs to exported to the client. Path should start with /vx and only
“a-zA-Z0-9_/.” characters are allowed in export_dir.

server [start|stop|status|switch]  Start, stop, or check the status of NFS resources. Server switch command will toggle active server from kernel NFS server (KNFS) to usermode Ganesha NFS server (GNFS) and vice versa.

stat show [nodename]  Display NFS statistics for nodename or all the nodes in the cluster.

stat reset [nodename]  Reset NFS statistics for nodename or all the nodes in the cluster to zero. Statistics are automatically reset to zero after reboot of a node. This command is not supported with GNFS.

share add nfsoptions export_dir [client]  Export the directory with the specified options. Clients may be specified in the following ways: 1. Single host
   Specify a host either by an abbreviated name recognized by the resolver, the fully qualified domain name, or an IP address.

   2. Netgroups
   Netgroups may be given as @group. Only the host part of each netgroup member is considered when checking for membership.

   3. IP networks
   You can also simultaneously export directories to all hosts on an IP (sub-) network. This is done by specifying an IP address and netmask pair as address/netmask where the netmask can be specified as a contiguous mask length. IPv4 or IPv6 addresses can be used.

If the client is not given, then the specified file system can be accessed or mounted by any client.

To re-export new options to an existing share, the new options will be updated after the command is run.

share delete export_dir [client]  Unexport the directory.

share show  List all of the exported resources.

show fs  List all of the online file systems and snapshots that can be exported.

10.1.4 EXAMPLES

Start the NFS server. If the NFS server is already started, the start command clears any faults and then tries to start the NFS server.

```
NFS> server start
..Success.
```

Display the status of the NFS server.

```
NFS> server status
NFS Status on nas_01 : ONLINE
NFS Status on nas_02 : ONLINE
```

Display the status of the Ganesha NFS server.

```
NFS> server status
GNFS Status on nas_01 : ONLINE
GNFS Status on nas_02 : ONLINE
```
Stop the NFS server. You will receive an error if you try to stop an already stopped NFS server.

```
NFS> server stop
..Success.
```

Display the list of FS/snapshot.

```
NFS> show fs
FS/Snapshot
========
fs1
```

Export the directory `/vx/fs1` to every host allowing asynchronous writes.

```
NFS> share add rw,async /vx/fs1
Exporting \/vx/fs1 with options rw,async
..Success.
```

Export the directory `/vx/fs1` using the krb5 security option.

```
NFS> share add sec=krb5 /vx/fs1
Exporting /vx/fs1 with options sec=krb5
Success.
```

Export a directory using krb5, krb5i, krb5p, and sys options. Different clients can use different levels of security in this case. Client A can mount with krb5, and client B can mount with krb5p. If no mount option is given at the client side, security to be chosen is negotiated, and the highest level of security is chosen. In this case, krb5p.

```
NFS> share add sec=krb5:krb5i:krb5p:sys /vx/fs1
Exporting /vx/fs1 with options sec=krb5:krb5i:krb5p:sys
Success.
```

Show the exported file system for KNFS.

```
NFS> share show
/vx/fs1 * (rw,async)
```

Show the exported file system for GNFS. To access GNFS shares of file system of type ‘largefs’, you must use the VIP that is associated with the share on the client. For shares of file systems of type other than ‘largefs’, user can use any VIP from the client to mount NFS shares. In the following example, IP 10.209.106.180 should be used to mount the NFS share on the client.

```
NFS> share show
/vx/fs1 * (rw,async) 10.209.106.180
```

Unexport the directory `/vx/fs1` from world.

```
NFS> share delete /vx/fs1
Removing export path \*:vx/fs1
..Success.
```

### 10.1.5 SEE ALSO

server(1), share(1), stat(1)
10.2 server

10.2.1 SYNOPSIS

server [start|stop|status|switch]

10.2.2 DESCRIPTION

The NFS server command starts, stops, switches, or checks the status of the NFS resources.

10.2.3 OPTIONS

server [start|stop|status|switch] Start, stop, or check the status of NFS resources. Server switch command will toggle active server from the kernel NFS server (KNFS) to usermode NFS-Ganesha (GNFS) or vice versa.

In case of the GNFS server, start command checks for the correct domain in the /etc/idmapd.conf file. If the domain is not set, NFSv4 ID mapping is not correct, and the command throws a warning to set the domain.

10.2.4 EXAMPLES

Start the NFS server. If the NFS server is already started, Veritas Access clears the faults (if any), and then tries to start the NFS server.

```
NFS> server start
..Success.
```

Display the status of the NFS server.

```
NFS> server status
NFS Status on nas_01 : ONLINE
NFS Status on nas_02 : ONLINE
```

Display the status of the Ganesha NFS server.

```
NFS> server status
GNFS Status on nas_01 : ONLINE
GNFS Status on nas_02 : ONLINE
```

Stop the NFS server. You will receive an error if you try to stop an already stopped NFS server.

```
NFS> server stop
..Success.
```

Switch the NFS server. You will receive an error if the NFS server is running.

```
NFS> server switch
This command will switch NFS server from GNFS to KNFS and will take time.
Do you want to continue (y/n): y
ACCESS nfs SUCCESS V-288-0 NFS server switch from GNFS to NFS successful. Please →
←start NFS service.
```
10.2.5 SEE ALSO

share(1), stat(1)
10.3 share

10.3.1 SYNOPSIS

share add nfsoptions export_dir [client]
share delete export_dir [client]
share show

10.3.2 DESCRIPTION

The NFS share commands add, delete, or display the NFS share.

10.3.3 OPTIONS

   nfsoptions  Comma-separated list of export options from the set {ro, rw, sync, async, secure, insecure, secure_locks, insecure_locks, root_squash, no_root_squash, wdelay, no_wdelay, subtree_check, no_subtree_check, nordirplus, fsid=<number>, sec=krb5:krb5i:krb5p:sys:none}. For example: ro,root_squash; rw,secure,no_root_squash. The default export options are {ro, sync, secure, secure_locks, root_squash, wdelay, no_subtree_check}. The “no_wdelay” option has no effect if “async” is also set. fsid could be any number between 1 and 1073741823. fsid must be unique among all exported paths.

   wdelay: For backwards-compatibility, the wdelay and no_wdelay options are still supported, but the options are being deprecated. The effective behavior is no_wdelay is used, even when wdelay is set. Clients can handle flushing of data using server COMMIT operations and UNSTABLE writes.

   export_dir  Path of the directory that needs to exported to the client. The path should start with /vx and only 'a-zA-Z0-9_/:-. characters are allowed in export_dir.

   share add nfsoptions export_dir [client]  Export the directory with the specified options. Clients may be specified in the following ways:

   1. Single host
      Specify a host either by an abbreviated name recognized by the resolver, the fully qualified domain name, or an IP address.

   2. Netgroups
      Netgroups may be given as @group. Only the host part of each netgroup member is considered when checking for membership.

   3. IP networks
      You can also simultaneously export directories to all hosts on an IP (sub-) network. This is done by specifying an IP address and netmask pair as address/netmask where the netmask can be specified as a contiguous mask length. IPv4 addresses or IPv6 addresses can be used.

If the client is not given, then the specified file system can be accessed or mounted by any client.

To re-export new options to an existing share, the new options will be updated after the command is run.

   share delete export_dir [client]  Unexport the directory.
\textbf{share show} List all of the exported resources. To access GNFS shares of file system of type ‘largefs’, you must use the VIP that is associated with the share on the client. For the shares of file systems of type other than ‘largefs’, you can use any VIP from the NFS client to mount the NFS shares.

### 10.3.4 EXAMPLES

Export the directory \texttt{/vx/fs1} to every host allowing asynchronous writes.

```
NFS> share add rw,async /vx/fs1
Exporting \*:/vx/fs1 with options rw,async
..Success.
```

Export the directory \texttt{/vx/fs1} using the krb5 security option. This is allowed only for GNFS.

```
NFS> share add sec=krb5 /vx/fs1
Exporting /vx/fs1 with options sec=krb5
Success.
```

Export the directory \texttt{/vx/fs1} using krb5, krb5i, krb5p, and sys options. This is allowed only for GNFS. Different clients can use different levels of security in this case. Client A can mount with krb5, and client B can mount with krb5p. If no mount option is given at the client side, security to be chosen is negotiated, and the highest level of security is chosen. In this case, krb5p.

```
NFS> share add sec=krb5:krb5i:krb5p:sys /vx/fs1
Exporting /vx/fs1 with options sec=krb5:krb5i:krb5p:sys
Success.
```

Show the exported file system for KNFS.

```
NFS> share show
/vx/fs1 * (rw,async)
```

Show the exported file system for GNFS. In the following example, IP 10.209.106.180 should be used to mount the share on the client if fs1 is largefs.

```
NFS> share show
/vx/fs1 * (rw,async) 10.209.106.180
```

Unexport the directory \texttt{/vx/fs1} from world.

```
NFS> share delete /vx/fs1
Removing export path \*:/vx/fs1
..Success.
```

### 10.3.5 SEE ALSO

server(1), stat(1)
10.4 show

10.4.1 SYNOPSIS

show fs

10.4.2 DESCRIPTION

The show fs command displays a list of all online file systems and snapshots that can be exported.

10.4.3 EXAMPLES

Display the list of file systems and snapshots.

NFS> show fs
FS/Snapshot
==========
fs1

10.4.4 SEE ALSO

share(1), server(1)
10.5 stat

10.5.1 SYNOPSIS

stat show [nodename]
stat reset [nodename]

10.5.2 DESCRIPTION

The NFS stat manages NFS statistics.

10.5.3 OPTIONS

stat show [nodename] Display NFS statistics for nodename or all nodes in the cluster.
stat reset [nodename] Reset NFS statistics for nodename or all the nodes in the cluster to zero.
Statistics are automatically reset to zero after reboot of a node. This command is not supported with GNFS.

10.5.4 EXAMPLES

Show NFS statistics for all nodes in the cluster.

NFS> stat show all
node_01
-------
Server rpc stats:
calls  badcalls  badclnt  badauth  xdrcall
0 0 0 0
Server nfs v3:
null  getattr  setattr  lookup  access  readlink
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0
read  write  create  mkdir  symlink  mknod
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0
remove  rmdir  rename  link  readdir  readdirplus
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0
fsstat  fsinfo  pathconf  commit
0 0% 0 0% 0 0% 0 0%
Server nfs v4:
null  compound
0 0% 0 0% 0 0%
Server nfs v4 operations:
op0-unused  op1-unused  op2-future  access
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0%
close  commit
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0%
create  delegpurge  delegreturn  getattr
0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0% 0 0%
link
node_02

Server rpc stats:
calls  badcalls  badclnt  badauth  xdrcall
     0      0       0        0       0

Server nfs v3:
null  getattr  setattr  lookup  access  readlink
     0         0         0         0         0         0
     0         0

read  write  create  mkdir  symlink  mknod
     0         0         0         0         0         0
     0         0

remove  rmdir  rename  link  readdir  readdirplus
     0         0         0         0         0         0
     0         0

fsstat  fsinfo  pathconf  commit
     0         0         0         0

Server nfs v4:
null  compound
     0         0
Show GNFS statistics for all the nodes in the cluster.

NFS> stat show all

<table>
<thead>
<tr>
<th>EXPORT PATH</th>
<th>PROTO</th>
<th>TYPE</th>
<th>REQ (MB)</th>
<th>XFER (MB)</th>
<th>TOTAL OPS</th>
<th>AVG LATENCY (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vx/fs1</td>
<td>NFSv3</td>
<td>READ</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>/vx/fs1</td>
<td>NFSv3</td>
<td>WRITE</td>
<td>48.00</td>
<td>48.00</td>
<td>48</td>
<td>11.85</td>
</tr>
<tr>
<td>/vx/fs1</td>
<td>NFSv4</td>
<td>READ</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
<td>0.00</td>
</tr>
<tr>
<td>/vx/fs1</td>
<td>NFSv4</td>
<td>WRITE</td>
<td>100.00</td>
<td>100.00</td>
<td>100</td>
<td>8.42</td>
</tr>
</tbody>
</table>

10.5. stat
Reset NFS statistics to zero on node_02.

NFS> stat reset node_02
Success.

10.5.5 SEE ALSO

share(1), server(1)
11. Object Access Commands

11.1 ObjectAccess

11.1.1 SYNOPSIS

account user show
bucket show [bucket_name]
group [set|show|unset]
server [enable|start|stop|status|disable]
set [ssl_enabled|pools|fs_size|fs_type]
unset pools pool1[,pool2,...]
map filesystem_path username
show

11.1.2 DESCRIPTION

The ObjectAccess commands are used to manage the object access service, to show the status of the service, to set and unset the default or group specific configuration, and to manage the buckets accessed using the Amazon S3 protocol.

The following are the steps to configure and use the Veritas object access service.

1. Set up the default runtime configuration options. You need to set at least one default pool. For example, objectaccess set pools slow_pool.
2. Enable the object access server.
3. Start the object access server.

The object access server creates a new file system for every new bucket. The type, size, and pools for the new file system should be configured correctly by using the object access set command. If the group set fs_sharing option is set to no, a new file system is created for the bucket every time. If the group set fs_sharing option is set to yes, then new buckets are created under the existing file system. If the administrator expects a large number of buckets to be created, the administrator can choose to share the same file system across all the users of the given group.
You cannot start the object access service until you have enabled it.

4. Configure NIS/LDAP/AD with Veritas Access and create keys for user authentication.

The object access server provides a custom REST-based API to create an access key and a secret key. The REST APIs use password-based authentication. It is recommended to always set `ssl_enabled` for the server. See the Veritas Access RESTful API Guide for more information.

5. Set up user groups.

The object access server can be configured to use specific configurations based on the requester user’s group. An administrator can override the file system type, size, pools, which should be used for a particular group. These group-specific options override the default options. For users that are not part of any pre-configured object access groups, the server uses the default configuration to create the file system.

Consider a pool, slow_pool, is created consisting of HDDs, and slow_pool is configured as the default pool. The default pool, slow_pool, applies to all users.

Consider a pool, fast_pool, is created consisting of only SSDs, and you want some users to use fast_pool for creating their buckets instead of the default slow_pool, then use the group options.

6. Use the object access server using an S3-API compatible client.

11.1.3 OPTIONS

`account user [show]` List the S3 users.

`bucket show [bucket_name]` List the buckets created by the S3 users.

`group [set|show|unset]` Groups allow an administrator to override the default file system configuration parameters. This gives fine control over how the object access server creates file systems and buckets for particular user groups. It is recommended to create new groups using the authentication server (NIS/LDAP/AD) based on your storage requirements and use them for this group configuration.

`server [enable|start|stop|status|disable]` Start, stop, or check the status of the object access service.

The server must be enabled before starting. Disabling the server deletes the object access configuration and user information database. All S3 buckets must be deleted before disabling the object access server.

`set [ssl_enabled|pools|fs_size|fs_type]` Set object access configurable and default file system options.

The object access server creates a new file system for every new bucket. Use the `set` command to create a new file system of a different configuration. The `ssl_enabled` option enables HTTPS access. The `pools` option lets you choose the pool on which the bucket has to be created. Use the `fs_size` option to set the default `fs_size` for the buckets.

`unset pools pool1[,pool2,...]` Remove pools from the default pool list. Removing all pools is not allowed as object access requires at least one default pool.

`show` List all the object access configurable options.

`map filesystem_path username` Map filesystem path as a bucket for a particular user. If filesystem path is not present then map command would create the directory and set the default S3 bucket permissions. The ownership to the bucket will be set to the user and it’s group. Filesystem path should not be in a directory inside exported nfs share or inside existing bucket. Bucket name will be same as a directory name.
11.1.4 EXAMPLES

Enable the object access service.

```
earth.ObjectAccess> server enable
100% [********************] Enabling ObjectAccess server.
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess server enabled.
```

Start the object access service.

```
earth.ObjectAccess> server start
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess started successfully.
```

Display the status of the object access service.

```
earth.ObjectAccess> server status
ObjectAccess Status on earth_01 : ONLINE
ObjectAccess Status on earth_02 : ONLINE
```

Stop the object access service.

```
earth.ObjectAccess> server stop
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess stopped successfully.
```

Disable the object access service.

```
earth.ObjectAccess> server disable
This operation will delete ObjectAccess authentication information, do you want to continue(y/n): y
100% [********************] Disabling ObjectAccess server.
```

Display the configuration of the object access service.

```
earth.ObjectAccess> show
Name             Value
----------------- ------------------------
Server Status    Disabled
Admin_URL        http://admin.earth:8144
S3_URL           http://s3.earth:8143
admin_port       8144
s3_port          8143
ssl              no
fs_size          20G
pools            pool1,pool2
fs_blksize       8192
fs_pdirenable    no
fs_encrypt       off
fs_type          mirrored
fs_nmirrors      2
fs_protection    disk
```

List the S3 users.

```
earth.ObjectAccess> account user show
AccessKey   UserName
----------------- ------------------------
MzhiNzR1NDQ1MDQ1YjB  user1
```
List the buckets created by the S3 users.

```
earth/ObjectAccess> bucket show
Bucket Name  Fs Name     Pool       Owner
------------------------ ============= =========== ================
nis-user1-group1bucket13 S3fs1489227391 pool-group1 nis-user1-group1
nis-user1-group1bucket12 S3fs1489224108 pool-s3_2 nis-user1-group1
nis-user1-group1bucket11 S3fs1489224886 pool-s3_2 nis-user1-group1
nis-user1-group1bucket14 S3fs1489227391 pool-group1 nis-user1-group1
nis-user1-group1bucket1   S3fs1489224561 pool-s3_2 nis-user1-group1
moonbucket1               S3fs1489224108 pool-s3_2 user1
nis-user1-group3bucket1   S3fs1489229942 pool-s3_2 nis-user1-group3
```

List the bucket details for the specific bucket.

```
earth/ObjectAccess> bucket show nis-user1-group1bucket13
Bucket Name  Fs Name     Pool       Owner
------------------------ ============= =========== ================
nis-user1-group1bucket13 S3fs1489227391 pool-group1 nis-user1-group1
```

Enable secure socket communication for the object access server.

```
earth/ObjectAccess> set ssl_enabled yes
ACCESS ObjectAccess INFO V-288-0 Set ssl-enabled successful.
ACCESS SSL INFO V-288-0 Note: Please restart the objectaccess server.
```

Set the default pool(s), which are used to create the file system while creating the buckets. This default pool can be overridden by setting up group-specific options by using the `set` command.

```
earth/ObjectAccess> set pools pool1,pool2
ACCESS ObjectAccess INFO V-288-0 Set pools successful. Please make sure the storage is provisioned as per the requirements of the layout.
```

Set the default file system size that should be used while creating the file system for a given bucket. This default `fs_size` can be overridden by setting up group-specific options by using the `set` command.

```
earth/ObjectAccess> set fs_size 10G
ACCESS ObjectAccess INFO V-288-0 Set operation successful.
```

Set the group’s pool mapping. In the following example, all the buckets of nis-group1 get created on pool-group1.

```
earth/ObjectAccess> group set pool nis-group1 pool-group1
ACCESS ObjectAccess INFO V-288-0 Set pool successful.
```

Set the group’s file system type.

```
earth/ObjectAccess> group set fs_type simple nis-group1 blksize=1024 pdir_enable=no encrypt=off
ACCESS ObjectAccess INFO V-288-0 Set pool successful.
```

Set the group’s file system size.

```
earth/ObjectAccess> group set fs_size nis-group1 5G
ACCESS ObjectAccess INFO V-288-0 Set fs_size successful.
```
Set the group’s file system sharing.

```
earth.ObjectAccess> group set fs_sharing nis-group1 yes
ACCESS ObjectAccess INFO V-288-0 Set fs_sharing successful.
```

Unset the group’s pool mapping.

```
earth.ObjectAccess> group unset pool nis-group1 pool-group1
ACCESS ObjectAccess INFO V-288-0 group unset pool Successful.
```

Unset the group’s fs_sharing.

```
earth.ObjectAccess> group unset fs_sharing nis-group1
ACCESS ObjectAccess INFO V-288-0 group unset fs_sharing Successful.
```

Unset the group’s fs_size.

```
earth.ObjectAccess> group unset fs_size nis-group1
ACCESS ObjectAccess INFO V-288-0 group unset fs_size Successful.
```

Show the group’s configuration details.

```
earth.ObjectAccess> group show
Group Name  Fs Sharing  Fs Size  Fs Type  Pool
==========  ===========  =======  =======  ===============
nis-group1  yes         5G       simple  pool-group1
```

Map file system path as bucket for a particular user.

```
earth.ObjectAccess> map /vx/fs1/dir1 s3user1
ACCESS ObjectAccess SUCCESS V-288-0 Successfully mapped bucket dir1 to s3user1.
```

11.1.5 SEE ALSO

account(1), group(1), bucket(1), server(1), show(1), set(1), unset(1), map(1)
11.2 account

11.2.1 SYNOPSIS

```
account user show
```

11.2.2 DESCRIPTION

The ObjectAccess account command is used to list the S3 users.

11.2.3 OPTIONS

```
account user show  List the S3 users.
```

11.2.4 EXAMPLES

List the S3 users.

```
earth.ObjectAccess> account user show
AccessKey     UserName
=----------------- =---------------
MzhiNzRlNDQ1MDQ1YjB user1
M2UzZmQzMTk1MjU2MDY nis-user1-group1
ZTMyYTR1YWMwNTE4ZDV nis-user1-group3
```

11.2.5 SEE ALSO

objectaccess(1)
11.3 bucket

11.3.1 SYNOPSIS

bucket show [bucket_name]

11.3.2 DESCRIPTION

The ObjectAccess bucket show command is used to list the buckets created by the S3 users.

11.3.3 OPTIONS

  bucket [show]  List the buckets created by the S3 users.

11.3.4 EXAMPLES

List the buckets created by the S3 users. For the buckets created on a scale-out fs, use the displayed IP to access the bucket. S3 buckets created on a scale-out file system must be accessed using a virtual-hosted-style URL (rather than the path-style URL) and the S3 client's DNS must be updated to this virtual IP address for the corresponding virtual-hosted-style URL. If a bucket scale-out-bucket1 is created by the S3 user, then its virtual-hosted-style URL would be scale-out-bucket1.s3.cluster_name:8143, where cluster_name is the Veritas Access cluster name and 8143 is the port on which the Veritas Access S3 server is running. For the buckets created on a non scale-out file system, the IP address is not applicable, as the bucket can be accessed using any VIP of the cluster.

```
earth.ObjectAccess> bucket show
Bucket Name      Fs Name        Pool(s)  Owner       IP
---------------- ============== =========== ================ =============
nis-user1-group1bucket1  S3fs1489227391 pool-group1 nis-user1-group1 -
nis-user1-group1bucket2  S3fs1489224108 pool-s3_2  nis-user1-group1 -
nis-user1-group1bucket11 S3fs1489224886 pool-s3_2  nis-user1-group1 -
nis-user1-group1bucket14 S3fs1489227391 pool-group1 nis-user1-group1 -
nis-user1-group1bucket1  S3fs1489224108 pool-s3_2  nis-user1-group1 -
moobucket1           S3fs1489224108 pool-s3_2  user1          -
nis-user1-group3bucket1 S3fs1489229942  pool-s3_2  nis-user1-group3 -
scale-out-bucket1     S3fs1489230130 pool-group2 nis-user1-group4  192.168.10.32
```

11.3.5 SEE ALSO

objectaccess(1)
11.4 group

11.4.1 SYNOPSIS

```bash
group set [fs_sharing|fs_size|fs_type|pools] group_name value
```

```bash
group show [group_name]
```

```bash
group unset group_name [fs_sharing|fs_size|fs_type|pool]
```

11.4.2 DESCRIPTION

The ObjectAccess group commands allow an administrator to override the default file system configuration parameters. This gives fine control over how the object access server creates file systems and buckets for particular user groups. It is recommended to create new groups using the authentication server (NIS/LDAP/AD) and use them for this group configuration.

11.4.3 OPTIONS

- `group set [fs_sharing|fs_size|fs_type|pools] group_name value` The `fs_sharing` option determines whether to create a new file system or to use an existing file system for creating the bucket. The `fs_size` and `fs_type` option allow you to set size and type of the file system for the group if any configuration parameters are not set. The `pools` option lets you choose the pool on which the bucket has to be created. If any configuration parameter is not set then it will pick from default configuration.

- `group show [group_name]` Lists group specific configurations for all the groups. If group name is specified, it will give all configuration details for that group.

- `group unset group_name [fs_sharing|fs_size|fs_type|pool]` Removes the option set for the specific group.

11.4.4 EXAMPLES

Set the group’s pool mapping. In the following example, all the buckets of nis-group1 get created on pool-group1.

```bash
earth.ObjectAccess> group set pool nis-group1 pool-group1
ACCESS ObjectAccess INFO V-288-0 Set pool successful.
```

Set the group’s file system type.

```bash
earth.ObjectAccess> group set fs_type simple nis-group1 blksize=1024 pdir_enable=no encrypt=off
ACCESS ObjectAccess INFO V-288-0 Set pool successful.
```

Set the group’s file system size.

```bash
earth.ObjectAccess> group set fs_size nis-group1 5G
ACCESS ObjectAccess INFO V-288-0 Set fs_size successful.
```

Set the group’s file system sharing.

```bash
earth.ObjectAccess> group set fs_sharing nis-group1 yes
ACCESS ObjectAccess INFO V-288-0 Set fs_sharing successful.
```
Unset the group’s pool mapping.

```bash
earth.ObjectAccess> group unset nis-group1 pool pool-group1
ACCESS ObjectAccess INFO V-288-0 group unset pool Successful.
```

Unset the group’s fs_sharing.

```bash
earth.ObjectAccess> group unset nis-group1 fs_sharing
ACCESS ObjectAccess INFO V-288-0 group unset fs_sharing Successful.
```

Unset the group’s fs_type.

```bash
earth.ObjectAccess> group unset nis-group1 fs_type
ACCESS ObjectAccess INFO V-288-0 group unset fs_type Successful.
```

Unset the group’s fs_size.

```bash
earth.ObjectAccess> group unset nis-group1 fs_size
ACCESS ObjectAccess INFO V-288-0 group unset fs_size Successful.
```

Show the group’s configuration details.

```bash
moon.ObjectAccess> group show
<table>
<thead>
<tr>
<th>Group Name</th>
<th>Fs Sharing</th>
<th>Fs Size</th>
<th>Fs Type</th>
<th>Pool(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>nis-group1</td>
<td>yes</td>
<td>5G</td>
<td>simple</td>
<td>pool-group1</td>
</tr>
</tbody>
</table>
```

```bash
moon.ObjectAccess> group show nis-group1
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>nis-group1</td>
</tr>
<tr>
<td>poollist</td>
<td>pool-group1</td>
</tr>
<tr>
<td>fs_sharing</td>
<td>yes</td>
</tr>
<tr>
<td>fs_size</td>
<td>5G</td>
</tr>
<tr>
<td>fs_type</td>
<td>simple</td>
</tr>
<tr>
<td>fs_blksize</td>
<td>1024</td>
</tr>
<tr>
<td>fs_pdirenable</td>
<td>no</td>
</tr>
<tr>
<td>fs_encrypt</td>
<td>off</td>
</tr>
<tr>
<td>fs_type</td>
<td>simple</td>
</tr>
</tbody>
</table>
```

### 11.4.5 SEE ALSO

`objectaccess(1)`
11.5 map

11.5.1 SYNOPSIS

map filesystem_path username

11.5.2 DESCRIPTION

Map the specific path as an S3 bucket for a particular user. The file system path can be either a directory inside a normal file system or an NFS exported path. If the specified path is not present, then the map command creates the directory and sets the default S3 bucket permissions. The ownership of the bucket is set to the user and it's group. The file system path should not be a directory inside the exported NFS share or the existing bucket. The bucket name is the same as the directory name. Admin can check the path mapping with the bucket show command.

11.5.3 OPTIONS

map filesystem_path username

Map filesystem_path as a S3 bucket for user username. Path can be any directory path inside the file system or nfs exported path. User can be any authenticated user from AD/LDAP/NIS.

11.5.4 EXAMPLES

Map the file system path in which directory is not present as an S3 bucket.

```
vmdollr> objectaccess map /vx/simple_fs/dir2 domain1/ad-user2
ACCESS ObjectAccess SUCCESS V-288-0 Successfully mapped bucket dir2 to domain1/ad-user2.
```

Map the file system path in which directory is already present as an S3 bucket.

```
vmdollr> objectaccess map /vx/simple_fs/dir6 user2
This operation will change the ownership of directory '/vx/simple_fs/dir6' to user user2' and will affect existing permissions. Do you want to continue (yes/no)? yes
ACCESS ObjectAccess SUCCESS V-288-0 Successfully mapped bucket dir6 to user2.
```

Map the nfs share path as an S3 bucket.

```
vmdollr> objectaccess map /vx/simple_fs/dir4 user2
This operation will change the ownership of directory '/vx/simple_fs/dir4' to user user2' and will affect existing permissions. Do you want to continue (yes/no)? yes
ACCESS ObjectAccess SUCCESS V-288-0 Successfully mapped bucket dir4 to user2.
```

11.5.5 SEE ALSO

objectaccess(1)
11.6 server

11.6.1 SYNOPSIS

server [enable|start|stop|status|disable]

11.6.2 DESCRIPTION

The ObjectAccess server commands are used to start, stop, or check the status of the object access server.

11.6.3 OPTIONS

server [enable|start|stop|status|disable]  Start, stop, or check the status of the object access service.

The server must be enabled before starting. Disabling the server deletes the object access configuration and user information database. All S3 buckets must be deleted before disabling the object access server.

11.6.4 EXAMPLES

Enable the object access service.

```
earth.ObjectAccess> server enable
100% [********************] Enabling ObjectAccess server.
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess server enabled.
```

Start the object access service.

```
exxearth.ObjectAccess> server start
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess started successfully.
```

Display the status of the object access service.

```
extart.ObjectAccess> server status
ObjectAccess Status on earth_01 : ONLINE
ObjectAccess Status on earth_02 : ONLINE
```

Stop the object access service.

```
extart.ObjectAccess> server stop
ACCESS ObjectAccess SUCCESS V-288-0 ObjectAccess stopped successfully.
```

Disable the object access service.

```
extart.ObjectAccess> server disable
This operation will delete ObjectAccess authentication information, do you want to continue(y/n): y
100% [********************] Disabling ObjectAccess server.
```

11.6.5 SEE ALSO

objectaccess(1)
11.7 set

11.7.1 SYNOPSIS

```
set [ssl_enabled|pools|fs_size|fs_type]
```

11.7.2 DESCRIPTION

The ObjectAccess commands are used to set object access configurable and default file system options.

11.7.3 OPTIONS

```
set [ssl_enabled|pools|fs_size|fs_type]
```

Set object access configurable and default file system options. The object access server creates a new file system for every new bucket. Use the set command to create a new file system of a different configuration. The `ssl_enabled` option enables HTTPS access. The `pools` option lets you choose the pool on which the bucket has to be created. Use the `fs_size` option to set the default file system size for the buckets. Use the `fs_type` option to choose the type of the file system that is created as part of bucket creation.

11.7.4 EXAMPLES

Set `ssl_enabled` to `yes` to have secure communication between the client and the server.

```
earth.ObjectAccess> set ssl_enabled yes
ACCESS ObjectAccess INFO V-288-0 Set ssl-enabled successful.
ACCESS SSL INFO V-288-0 Note: Please restart the objectaccess server.
```

Set `ssl_enabled` to `no` if you do not want secure communication.

```
earth.ObjectAccess> set ssl_enabled no
ACCESS ObjectAccess INFO V-288-0 Set ssl-enabled successful.
ACCESS SSL INFO V-288-0 Note: Please restart the objectaccess server.
```

Set the default pool(s), which are used to create the file system while creating the buckets. This default pool can be overridden by setting up group-specific options by using the `set` command.

```
earth.ObjectAccess> set pools pool1
ACCESS ObjectAccess INFO V-288-0 Set pools successful. Please make sure the storage is provisioned as per the requirements of the layout.
```

Set the default `fs_type` to a mirrored layout with 2 mirrors.

```
earth.ObjectAccess> set fs_type mirrored 2 protection=pool blksize=1024 pdir_=enable=no encrypt=off
ACCESS ObjectAccess INFO V-288-0 Set fs_type mirrored successful.
```

Set the default `fs_type` to scale-out fs simple layout.

```
earth.ObjectAccess> set fs_type largefs simple
ACCESS ObjectAccess INFO V-288-0 Set fs_type successful. Please make sure the storage is provisioned as per the requirements of the layout.
```
Set the default file system size that should be used while creating the file system for a given bucket. This default \texttt{fs\_size} can be overridden by setting up group-specific options by using the \texttt{set} command.

\begin{verbatim}
earth.ObjectAccess> set fs_size 10G
ACCESS ObjectAccess INFO V-288-0 Set operation successful.
\end{verbatim}

\section*{11.7.5 SEE ALSO}

\texttt{objectaccess(1), unset(1)}
11.8 show

11.8.1 SYNOPSIS

show

11.8.2 DESCRIPTION

The ObjectAccess show command is used to list all the object access service configurable options.

11.8.3 OPTIONS

   show  List all the object access configurable options.

11.8.4 EXAMPLES

Display the configuration of the object access service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Status</td>
<td>Disabled</td>
</tr>
<tr>
<td>Admin_URL</td>
<td><a href="http://admin.earth:8144">http://admin.earth:8144</a></td>
</tr>
<tr>
<td>S3_URL</td>
<td><a href="http://s3.earth:8143">http://s3.earth:8143</a></td>
</tr>
<tr>
<td>admin_port</td>
<td>8144</td>
</tr>
<tr>
<td>s3_port</td>
<td>8143</td>
</tr>
<tr>
<td>ssl</td>
<td>no</td>
</tr>
<tr>
<td>fs_size</td>
<td>20G</td>
</tr>
<tr>
<td>pools</td>
<td>pool1,pool2</td>
</tr>
<tr>
<td>fs_blksize</td>
<td>8192</td>
</tr>
<tr>
<td>fs_pdirenable</td>
<td>no</td>
</tr>
<tr>
<td>fs_encrypt</td>
<td>off</td>
</tr>
<tr>
<td>fs_type</td>
<td>mirrored</td>
</tr>
<tr>
<td>fs_nmirrors</td>
<td>2</td>
</tr>
<tr>
<td>fs_protection</td>
<td>disk</td>
</tr>
</tbody>
</table>

11.8.5 SEE ALSO

objectaccess(1), set(1), unset(1)
11.9 unset

11.9.1 SYNOPSIS

unset pools pool1[,pool2,...]

11.9.2 DESCRIPTION

The ObjectAccess unset command is used to unset the configuration of the object access service.

11.9.3 OPTIONS

unset pools pool1[,pool2,...] Remove pools from the default pool list. If any bucket is present in that pool, then the unset command fails for that pool. Removing all the pools is not allowed as the object access service requires at least one default pool.

11.9.4 EXAMPLES

Unset the pool mapping.

earth.ObjectAccess> unset pools pool-group1
ACCESS ObjectAccess INFO V-288-0 Unset pools successful.

11.9.5 SEE ALSO

objectaccess(1), set(1)
12.1 openstack

12.1.1 SYNOPSIS

cinder configure export_dir
cinder service start
cinder service status
cinder share add export_dir world\client
cinder share delete export_dir world\client
cinder share show
manila configure pool_name
manila resource export pool_name
manila resource delete pool_name
manila resource list

12.1.2 DESCRIPTION

The openstack commands configure Veritas Access to work with OpenStack Cinder or Manila. The OpenStack cinder share commands add, delete, or display the NFS share. OpenStack cinder configure command displays all the configuration changes that need to be done on the Cinder node to access the Veritas Access storage as a volume backend from Cinder. OpenStack manila resource command exports/unexports any existing storage pools of Veritas Access to OpenStack Manila.

12.1.3 OPTIONS

- **export_dir** Path of the directory that needs to be exported to the client. The directory path should start with /vx and only ‘a-zA-Z0-9_/@+=.-’ characters are allowed in export_dir.

- **client** Export the directory with the specified options. Clients may be specified in the following ways:
1. Single host
   Specify a host either by an abbreviated name recognized by the resolver, the fully qualified
domain name, or an IP address.

2. Netgroups
   Netgroups may be given as @group. Only the host part of each netgroup member is considered
   when checking for membership.

3. IP networks
   You can also simultaneously export directories to all hosts on an IP (sub-) network. This is
done by specifying an IP address and netmask pair as address/netmask where the netmask can
be specified as a contiguous mask length. IPv4 or IPv6 addresses can be used.

   world With this option, the specified file system will be accessed or mounted by any client. To re-export
   new options to an existing share, the new options will be updated after the command is run.

   pool_name Existing storage pool that has been exported to Manila.

   cinder configure export_dir Display all the configuration changes that need to be done on the
   OpenStack Controller node. After making these modifications on the OpenStack Controller node,
you can use the Veritas Access storage as a volume backend.

   cinder service start Start the OpenStack Cinder service on Veritas Access.

   cinder service status Display the status of the OpenStack Cinder service on Veritas Access.

   cinder share add export_dir client Share and export the file system export-dir. After issuing this
   command, OpenStack Cinder will be able to mount the exported file system using NFS.

   cinder share delete export_dir client Delete (or unshare) the exported file system. Share and
   export /vx/fs1 using NFS to all the clients.

   cinder export_dir client Delete (or unshare) the exported file system. Share and export /vx/fs1 using
   NFS to all the clients.

   manila configure pool_name Display all the configuration changes that need to be done on the
   OpenStack Controller node, given an exported pool.

   manila resource export pool_name Export existing pool pool_name to the Veritas Access
   OpenStack Manila driver.

   manila resource delete pool_name Unexport the exported pool.

   manila resource list List all the Veritas Access resources created or exported by or to the
   Manila driver.

12.1.4 EXAMPLES

OPENSTACK> configure /vx/fs1

To create a new volume backend ACCESS_HDD in OpenStack Cinder

Make the following changes on the OpenStack controller node and restart the Cinder driver.

Add the following configuration entries in the /etc/cinder/cinder.conf file:
In the [DEFAULT] section:

```
enabled_backends=access-1
```

At the end of all the sections:

```
[access-1]
volume_driver=cinder.volume.drivers.veritas_cnfs.VeritasCNFSDriver
volume_backend_name=ACCESS_HDD
nfs_shares_config=/etc/cinder/access_share_hdd
nfs_mount_point_base=/cinder/cnfs/cnfs_sata_hdd
nfs_sparsed_volumes=True
nfs_disk_util=df
nfs_mount_options=nfsvers=3
```

Append the following in the `/etc/cinder/access_share_hdd` file:

```
vip:/vx/fs1
```

Use one of the following virtual IPs for `vip`:

192.1.1.190
192.1.1.191
192.1.1.192
192.1.1.193

OPENSTACK> cinder service start
..Success.

OPENSTACK> cinder service status
NFS Status on access_01 : ONLINE
NFS Status on access_02 : ONLINE

OPENSTACK> cinder share add /vx/fs1 world
Exporting /vx/fs1 with options rw,no_root_squash
Success.

OPENSTACK> cinder share delete /vx/fs1 world
Removing export path \*:vx/fs1
Success.

OPENSTACK> cinder share add /vx/fs1 world
Exporting /vx/fs1 with options rw,no_root_squash
Success.

OPENSTACK> manila configure pool1

To create a new share backend va-share1 in OpenStack Manila

Make the following changes on the OpenStack controller node and restart the Manila driver. Add the following configuration entries in the `/etc/manila/manila.conf` file:
In the [DEFAULT] section:

```
#####
enabled_backends=va-share1
#####
```

At the end of all the sections:

```
#####
[va-share1]
share_driver= manila.share.drivers.veritas.veritas_isa.ACCESSShareDriver
driver_handles_share_servers = False
share_backend_name = va-share1
va_server_ip = 10.182.96.179
va_port = 14161
va_ssl = False
va_fstype = simple
va_user = root
va_pwd = password
va_pool = pool1
#####
```

```
OPENSTACK> manila resource export pool1
ACCESS Manila SUCCESS V-288-0 Pool exported to Manila.

OPENSTACK> manila resource delete pool1
ACCESS Manila SUCCESS V-288-0 Pool removed from exported list.

OPENSTACK> manila resource list
Pools exported to Manila:
    pool1

FS created by Manila:
    0B54F556-ACE40746
    F4793495-227F6C9B

FS snapshots created by Manila:
    701C1975-AC635AAF

NFS shares exported by Manila:
    /vx/0B54F556-ACE40746
    /vx/0B54F556-ACE40746
```

### 12.1.5 SEE ALSO

cinder(1), manila(1)
12.2 cinder

12.2.1 SYNOPSIS

configure export_dir
service start
cinder service status
cinder share add export_dir world|client
cinder share delete export_dir world|client
cinder share show

12.2.2 DESCRIPTION

The cinder configure command displays all the configuration changes that need be done on the OpenStack Cinder node to access Veritas Access storage as a volume backend from OpenStack Cinder. Only after making these modifications on the OpenStack Cinder node, Cinder can use the Veritas Access share as a volume backend.

The cinder service start command starts the NFS service. NFS service has to be started as OpenStack service relies on it. The cinder service status command displays the status of the OpenStack service. If the NFS service is up, the OpenStack service is up.

The cinder service share commands add, delete, or display the NFS share. The OpenStack Cinder node can NFS mount a particular share only after issuing the add command.

Note: The Veritas Access server includes the Veritas Access OpenStack Cinder driver, which is a Python script.

The OpenStack Cinder driver is located at /opt/VRTSnas/scripts/OpenStack/veritas_cnfs.py on the Veritas Access server. If you are using the Python 2.6 release, copy the veritas_cnfs.py file to /usr/lib/python2.6/site-packages/cinder/volume/drivers/veritas_cnfs.py on the OpenStack controller node. If you are using the Python 2.7 release, copy the veritas_cnfs.py file to /usr/lib/python2.7/site-packages/cinder/volume/drivers/veritas_cnfs.py on the OpenStack controller node.

12.2.3 OPTIONS

export_dir Path of the directory that needs to be exported to the client. The directory path should start with /vx and only 'a-zA-Z0-9_/@+=.:-' characters are allowed in export_dir.

client Export the directory with the specified options. Clients may be specified in the following ways:

1. Single host
   Specify a host either by an abbreviated name recognized by the resolver, the fully qualified domain name, or an IP address.

2. Netgroups
   Netgroups may be given as @group. Only the host part of each netgroup member is considered when checking for membership.

3. IP networks
   You can also simultaneously export directories to all hosts on an IP (sub-) network. This is done by specifying an IP address and netmask pair as address/netmask where the netmask can be specified as a contiguous mask length. IPv4 or IPv6 addresses can be used.
world With this option, the specified file system will be accessed or mounted by any client.

To re-export new options to an existing share, the new options will be updated after the command is run.

cinder configure export_dir Display all the configuration changes that need to be done on the
OpenStack Cinder node. Only after these modifications on the OpenStack Cinder node, OpenStack
Cinder can use the Veritas Access storage as a volume backend.

cinder service start Start the cinder service on Veritas Access.

cinder service status Display the status of cinder service on Veritas Access.

cinder share add export_dir client Share and export the file system export-dir to client. Here
client is OpenStack controller node. After issuing this command, OpenStack Cinder will be able
to mount the exported file system using NFS. By default the file system export-dir is exported with
no_root_squash option.

cinder share add export_dir world Share and export the file system export-dir to all the clients.
After issuing this command, any node will be able to mount the exported file system using NFS.

cinder share delete export_dir client Delete (or unshare) the exported file system. Share and
export /vx/fs1 using NFS to all the clients.

cinder share delete export_dir world Unexport the exported file system to all clients. If a file
system is exported specifically to some clients, those clients would still access the file system.

12.2.4 EXAMPLES

OPENSTACK> cinder configure /vx/fs1

To create a new volume backend ACCESS_HDD in Cinder

Make the following changes on the OpenStack controller node and restart the Cinder driver.

Add the following configuration entries in the /etc/cinder/cinder.conf file: In the [DEFAULT] section:

```
#####
enabled_backends=access-1
#####
```

At the end of all the sections:

```
#####
[access-1]
volume_driver=cinder.volume_drivers.veritas_cnfs.VeritasCNFSDriver
volume_backend_name=ACCESS_HDD
nfs_shares_config=/etc/cinder/access_share_hdd
nfs_mount_point_base=/cinder/cnfs/cnfs_sata_hdd
nfs_sparse_volumes=True
nfs_disk_util=df
nfs_mount_options=nfsvers=3
#####
```

Append the following in the /etc/cinder/access_share_hdd file:

```
#####
vip:/vx/fs1
#####
```
Use one of the following virtual IPs for vip.

192.1.1.190
192.1.1.191
192.1.1.192
192.1.1.193

OPENSTACK> cinder service start
..Success.

OPENSTACK> cinder service status
NFS Status on access_01 : ONLINE
NFS Status on access_02 : ONLINE

OPENSTACK> cinder share add /vx/fs1 world
Exporting /vx/fs1 with options rw,no_root_squash
Success.

OPENSTACK> cinder share delete /vx/fs1 world
Removing export path */vx/fs1
Success.

OPENSTACK> cinder share add /vx/fs1 world
Exporting /vx/fs1 with options rw,no_root_squash
Success.

OPENSTACK> cinder share show
/vx/fs1 * (rw,no_root_squash)
12.3 manila

12.3.1 SYNOPSIS

manila resource export pool_name
manila resource delete pool_name
manila resource list
manila configure pool_name

12.3.2 DESCRIPTION

These commands configure Veritas Access to work with OpenStack Manila. manila configure command displays all the configuration changes that need to be done on the OpenStack controller node for the Manila service to communicate with Veritas Access for share creation and management.

The Manila resource export command exports any existing storage pools of Veritas Access to OpenStack Manila. The manila resource delete command unexports the exported pool provided to OpenStack. Veritas Access keeps record of all the shares, snapshots and NFS exports created by OpenStack manila driver, resource list displays all the resources created by the Manila driver.

Note: The Veritas Access server includes the Veritas Access OpenStack Manila driver, which is a Python script. The OpenStack Manila driver is located at /opt/VRTSnas/scripts/OpenStack/veritas/veritas_isa.py on the Veritas Access server. If you are using the Python 2.6 release, copy the veritas folder to /usr/lib/python2.6/site-packages/manila/share/drivers/ on the OpenStack controller node. If you are using the Python 2.7 release, copy the veritas folder to /usr/lib/python2.7/site-packages/manila/share/drivers/ on the OpenStack controller node.

manila configure pool_name Display all the configuration changes that need to be done on the OpenStack Controller node.

manila resource export pool_name Export existing pool pool_name to the Veritas Access OpenStack Manila driver.

manila resource delete pool_name Unexport the exported pool.

manila resource list List all the Veritas Access resources created or exported by or to the Manila driver.

12.3.3 EXAMPLES

Display all the configuration changes that need to be done on the OpenStack controller node to make pool1 as the share backend.

OPENSTACK> manila configure pool1

To create a new share backend va-share1 in OpenStack Manila

Make the following changes on OpenStack controller node and restart the Manila driver Add the following configuration entries in the /etc/manila/manila.conf file:
In the [DEFAULT] section:

```bash
#####
enabled_backends=va-share1
#####
```

At the end of all the sections:

```bash
#####
[va-share1]
share_driver= manila.share.drivers.veritas.veritas_isa.ACCESSShareDriver
driver_handles_share_servers = False
share_backend_name = va-share1
va_server_ip = 10.182.96.179
va_port = 14161
va_ssl = False
va_fstype = simple
va_user = root
va_pwd = password
va_pool = pool1
#####
```

```bash
OPENSTACK> manila resource export pool1
ACCESS REST SUCCESS V-288-1397 Export pool pool1 to REST server.

OPENSTACK> manila resource delete pool1
ACCESS REST SUCCESS V-288-1397 Removing exported pool pool1 from REST server.

OPENSTACK> manila resource list
Pools exported to Manila:
  pool1

FS created by Manila:
  0B54F556-ACE40746
  F4793495-227F6C9B

FS snapshots created by Manila:
  701C1975-AC635AAF

NFS shares exported by Manila:
  /vx/0B54F556-ACE40746
  /vx/0B54F556-ACE40746
```
13.1 report

13.1.1 SYNOPSIS

e-mail show [group]
e-mail add email-address filter group severity group
    [command-specific-options]
e-mail del email-address filter group severity group
    [command-specific-options]
e-mail get
e-mail set [email-server] [email-user]
event get dup-frequency
event get dup-number
event set dup-frequency number
event set dup-number number
showevents [number_of_events]
syslog add syslog-server-ipaddr
syslog delete syslog-server-ipaddr
syslog set filter severity value
syslog get filter severity
syslog show
snmp add snmp-mgmtserver-ipaddr
snmp delete snmp-mgmtserver-ipaddr
snmp set filter severity value
snmp get filter severity
snmp show
snmp exportmib url
exportevents url

13.1.2 DESCRIPTION

The report commands configure the notifications of events. The notifications are based on email notifications, SNMP traps, and passing a syslog of the events to the external syslog server. The commands also support showing the recent events. These events are centrally located.

13.1.3 OPTIONS

**email show [group]**  Show email groups or show an email group’s details.

**email add email-address|filter|group|severity group [command-specific-options]**  Add an email group, or add an email address, filter, or severity to an email group.

**email del email-address|filter|group|severity group [command-specific-options]**  Delete an email group, or delete an email-address, filter, or severity from an email group.

**email get**  Get the details of the configured external email server.

**email set [email-server] [email-user]**  Set the details of an external email server. If email-server and email-user are not specified, previously configured settings are deleted.

**event get dup-frequency**  View the time interval in which only one event (of duplicate events) is sent for notifications.

**event get dup-number**  View the number of duplicate events to ignore during notifications.

**event set dup-frequency number**  Set the time interval in which only one event (of duplicate events) is sent for notifications.

**event set dup-number number**  Set the number of duplicate events to ignore during notifications.

**showevents [number_of_events]**  Display the latest events.

**syslog add syslog-server-ipaddr**  Add an external syslog server.

**syslog delete syslog-server-ipaddr**  Delete a syslog server from the configured syslog servers.

**syslog set filter value**  Set the filter for the syslog notifications. Events matching with given filter are sent for notifications.

**syslog set severity value**  Set the severity for syslog notifications. Events having the same or higher severity are sent for notifications.

**syslog get filter|severity**  Get the values of the configured settings.

**syslog show**  Display the current list of external syslog servers.

**snmp add snmp-mgmtserver-ipaddr**  Add an SNMP management server.

**snmp delete snmp-mgmtserver-ipaddr**  Delete an already configured SNMP management server.

**snmp set filter value**  Set the filter for SNMP notifications. Events matching with given filter are sent for notifications.

**snmp set severity value**  Set severity for SNMP notifications. Events having the same or higher severity are sent for notifications.
**snmp get filter|severity**  Get the values of the configured settings.

**snmp show**  Display the current list of SNMP management servers.

**snmp exportmib [url]**  Upload the SNMP MIB file to a given URL. The URL supports FTP and SCP. If the URL specifies the remote directory, the default file name is access.mib.txt.

**exportevents [url]**  Export the events in syslog format to a given URL. The URL supports FTP and SCP. If the URL specifies a remote directory, the default file name is access_event.log when exporting the events.

### 13.1.4 EXAMPLES

Add an email group.

```
Report> email add group root
OK Completed
```

Add an email address to the group root.

```
Report> email add email-address root adminuser@localhost
OK Completed
```

Add a filter to an email group.

```
Report> email add filter root storage
OK Completed
```

Add a severity to an email group.

```
Report> email add severity root debug
OK Completed
```

Delete an existing email address from the email group.

```
Report> email del email-address root testuser@localhost
OK Completed
```

Try to delete a non-existent email address from the email group.

```
Report> email del email-address root testuser@localhos
ACCESS email del email-address ERROR V-288-50 Cannot remove email-address, it doesn't exist.
```

Set the details of the external email server.

```
Report> email set smtp.veritas.com adminuser
Enter password for user 'adminuser': ********
OK Completed
```

Get the details of the external email server.

```
Report> email get
E-Mail Server: smtp.veritas.com
E-Mail Username: adminuser
E-mail User's Password: ********
OK Completed
```

13.1. report
List the current configured email groups.

```
Report> email show
root
OK Completed
```

Display configuration of email group root.

```
Report> email show root
Group Name: root
Severity of the events: info,debug
Filter of the events: all,storage
Email addresses in the group: adminuser@localhost
OK Completed
```

View the duplicate events frequency.

```
Report> event get dup-frequency
Duplicate events frequency (in seconds): 60 (default)
OK Completed
```

View the number of duplicate events.

```
Report> event get dup-number
Duplicate number of events: 5 (default)
OK Completed
```

Set the duplicate events frequency to 120 seconds.

```
Report> event set dup-frequency 120
OK Completed
```

Set the number of duplicate events to 10.

```
Report> event set dup-number 10
OK Completed
```

View the newly set duplicate events frequency.

```
Report> event get dup-frequency
Duplicate events frequency (in seconds): 120
OK Completed
```

View the newly set number of duplicate events.

```
Report> event get dup-number
Duplicate number of events: 10
OK Completed
```

Display the last 10 events

```
Report> showevents 10
....... OK Completed
```

Add a new syslog server
Delete a configured syslog server.

```
Report> syslog delete syslog2.veritas.com
OK Completed
```

Show the configured syslog servers.

```
Report> syslog show
Configured syslog servers: syslog1.veritas.com, syslog2.veritas.com
OK Completed
```

Set the syslog events filter.

```
Report> syslog set filter storage
OK Completed
```

Get the configured syslog events filter.

```
Report> syslog get filter
Filter for the events: storage
OK Completed
```

Set the syslog events severity.

```
Report> syslog set severity err
OK Completed
```

Get the configured syslog events’ severity.

```
Report> syslog get severity
Severity of the events: err
OK Completed
```

Add a new SNMP management server.

```
Report> snmp add mgmtserv1.veritas.com
OK Completed
```

Delete a configured SNMP management server.

```
Report> snmp delete mgmtserv2.veritas.com
OK Completed
```

Pass invalid value for the SNMP server deletion.

```
Report> snmp delete mgmtserv22.veritas.com
ACCESS snmp delete ERROR V-288-26 Cannot delete SNMP management server, it doesn'texist.
```

Show configured SNMP management servers.

```
Report> snmp show
Configured SNMP management servers: mgmtserv1.veritas.com, mgmtserv2.veritas.com
OK Completed
```
Upload the SNMP MIB file:

```
Report> snmp exportmib scp://admin@server1.veritas.com:/tmp/access_mib.txt
Password: *****
OK Completed
```

Upload the events file in syslog format:

```
Report> exportevents scp://root@server1.veritas.com:/exportevents/event.1
Password: *****
OK Completed
```

Set the SNMP events filter:

```
Report> snmp set filter all
OK Completed
```

Get the configured SNMP events filter:

```
Report> snmp get filter
Filter for the events: all
OK Completed
```

Set the SNMP events’ severity:

```
Report> snmp set severity info
OK Completed
```

Get the configured SNMP events’ severity:

```
Report> snmp get severity
Severity of the events: info
OK Completed
```

**13.1.5 SEE ALSO**

email(1), exportevents(1), showevents(1), snmp(1), syslog(1), event(1)
13.2 email

13.2.1 SYNOPSIS

e-mail show [group]
e-mail add email-address|filter|group|severity group
   [command-specific-options]
e-mail del email-address|filter|group|severity group
   [command-specific-options]
e-mail get

e-mail set [email-server] [email-user]

13.2.2 DESCRIPTION

The report e-mail commands configure email notifications of events. These commands support adding email groups, adding filters to the group, adding email addresses to the email group, adding event severity to the group, and configuring an external email server for sending the event notification emails.

13.2.3 OPTIONS

  group Name of the group to create, or to add email addresses.

  email-server IP address or hostname of the external email server. IPv6 address should be enclosed by square brackets [ ].

  email-user Username of the external email server.

  email show [group] Show email groups or show an email group’s details.

  email add email-address|filter|group|severity group [command-specific-options] Add an email group, or add an email address, filter, or severity to an email group.

  email del email-address|filter|group|severity group [command-specific-options] Delete an email group, or delete an email-address, filter, or severity from an email group.

  email get Get the details of the configured external email server.

  email set [email-server] [email-user] Set the details of external email server. If email-server and email-user are not specified, previously configured settings will be deleted.

13.2.4 EXAMPLES

Add an email group.

Report> email add group root
OK Completed

Add an email address to the group root.

Report> email add email-address root adminuser@localhost
OK Completed

13.2. email

195
Add a filter to an email group.

```
Report> email add filter root storage
OK Completed
```

Add a severity to an email group.

```
Report> email add severity root debug
OK Completed
```

Delete an existing email address from the email group.

```
Report> email del email-address root testuser@localhost
OK Completed
```

Try to delete a non-existant email address from the email group.

```
Report> email del email-address root testuser@localhos
ACCESS email del email-address ERROR V-288-50 Cannot remove email-address, it doesn't exist.
```

Set the details of the external email server.

```
Report> email set smtp.veritas.com adminuser
Enter password for user 'adminuser': ********
```

Get the details of the external email server.

```
Report> email get
E-Mail Server: smtp.veritas.com
E-Mail Username: adminuser
E-mail User's Password: ********
OK Completed
```

List the current configured email groups.

```
Report> email show
root
OK Completed
```

Display configuration of email group root.

```
Report> email show root
Group Name: root
Severity of the events: info,debug
Filter of the events: all,storage
Email addresses in the group: adminuser@localhost
OK Completed
```

**13.2.5 SEE ALSO**

exportevents(1), showevents(1), snmp(1), syslog(1), event(1)
13.3 event

13.3.1 SYNOPSIS

event get dup-frequency
event get dup-number
event get log-scan-frequency
event get from-address
event set dup-frequency number
event set dup-number number
event set log-scan-frequency frequency
event set from-address from-email-address

13.3.2 DESCRIPTION

The report event command configures the settings for event reporting.

13.3.3 OPTIONS

  event get dup-frequency View the time interval in which only one event (of duplicate events) is sent for notifications.
  event get dup-number View the number of duplicate events to ignore during notifications.
  event get log-scan-frequency View the log scan frequency.
  event get from-address View the from email address when sending email to user. Set the from-address to default cluster_name@domain_name if set to empty
  event set dup-frequency number Set the time interval in which only one event (of duplicate events) is sent for notifications.
  event set dup-number number Set the number of duplicate events to ignore during notifications.
  event set log-scan-frequency frequency Set the time interval in which the event notify process scan /var/log/messages.
  event set from-address from-email-address Set the from email address when sending email to user.

13.3.4 EXAMPLES

View the duplicate events frequency.

```
Report> event get dup-frequency
Duplicate events frequency (in seconds): 60 (default)
Command completed successfully
```

View the number of duplicate events.
Report> event get dup-number
Duplicate number of events: 5 (default)
Command completed successfully

View the log scan frequency.

Report> event get log-scan-frequency
Log scan frequency (in seconds): 120 (default)
Command completed successfully

View the from email address.

Report> event get from-address
Email from address: EXAMPLE@access.smtc.com (default)
Command completed successfully

Set the duplicate events frequency to 120 seconds.

Report> event set dup-frequency 120
Command completed successfully

Set the number of duplicate events to 10.

Report> event set dup-number 10
Command completed successfully

Set the log scan frequency to 30.

Report> event set log-scan-frequency 30
Command completed successfully

Set the from email address to testaddr@veritas.com.

Report> event set from-address testaddr@veritas.com
Command completed successfully

View the newly set duplicate events frequency.

Report> event get dup-frequency
Duplicate events frequency (in seconds): 120
Command completed successfully

View the newly set number of duplicate events.

Report> event get dup-number
Duplicate number of events: 10
Command completed successfully

View the newly set log scan frequency.

Report> event get log-scan-frequency
Log scan frequency (in seconds): 30
Command completed successfully

View the newly set from email address.
Report> event get from-address
Email from address: testaddr@veritas.com
Command completed successfully

13.3.5 SEE ALSO

e-mail(1), exportevents(1), showevents(1), snmp(1), syslog(1)
13.4 exportevents

13.4.1 SYNOPSIS

exportevents url

13.4.2 DESCRIPTION

The report exportevents command exports events in syslog format to the specified URL.

13.4.3 OPTIONS

url URL location to upload the events file in syslog format.

exportevents url Export the events in syslog format to the specified URL. URL supports FTP and SCP. If the URL specifies the remote directory, the default filename is access_event.log.

13.4.4 EXAMPLES

Upload the events file in syslog format.

```
Report> exportevents scp://root@server1.veritas.com:/exportevents/event.1
Password:
File successfully exported to remote location
scp://root@10.209.133.242:/root/event.1
```

13.4.5 SEE ALSO

email(1), snmp(1), syslog(1), showevents(1), event(1)
13.5 showevents

13.5.1 SYNOPSIS

showevents [number_of_events]

13.5.2 DESCRIPTION

The report showevents command displays the latest events.

13.5.3 OPTIONS

number_of_events  Number of events to display. Entering 0 shows all of the events.

showevents [number_of_events]  Display latest events.

13.5.4 EXAMPLES

Display the last 10 events:

```
Report> showevents 10
November 12 17:30:24 [test_01,info,root] Disk list detail completed
November 12 17:30:35 [test_01,info,root] Disk list types completed
November 12 17:30:41 [test_01,info,root] Checked status of IO Fencing on the coordinator disks
November 12 17:30:54 [test_01,info,root] Disk list stats completed
November 12 17:32:20 [test_01,info,root] CIFS> share show
November 12 17:35:47 [test_01,alert,master] Could not connect
November 12 17:36:56 [test_01,info,test] Notification daemon started.
November 12 17:38:03 [test_01,alert,master] ERROR
November 12 17:38:17 [test_01,alert,master] Could not connect
November 12 17:38:54 [test_01,info,master] ping completed
......
```

13.5.5 SEE ALSO

email(1), exportevents(1), snmp(1), syslog(1), event(1)
13.6 snmp

13.6.1 SYNOPSIS

snmp add snmp-mgmtserver-ipaddr [community_string]
snmp delete snmp-mgmtserver-ipaddr
snmp set filter|severity value
snmp get filter|severity
snmp show
snmp exportmib url

13.6.2 DESCRIPTION

The report `snmp` command configures SNMP management servers and filter for notifications, and severity of notifications. The event notifications matching configured severity and filter are sent as SNMP traps to the servers configured with these commands.

13.6.3 OPTIONS

- **snmp-mgmtserver-ipaddr** Host name or IP address of the SNMP management server.
- **url** URL where to upload the SNMP MIB file.
- **value** Value of the variable to set.

- **snmp add snmp-mgmtserver-ipaddr [community_string]** Add an SNMP management server. The default community_string is ‘public’.
- **snmp delete snmp-mgmtserver-ipaddr** Delete an already configured SNMP management server.
- **snmp set filter value** Set filter for snmp notifications. Events matching with given filter will be sent for notifications.
- **snmp set severity value** Set severity for snmp notifications. Events having same or higher severity will be sent for notifications.
- **snmp get filter|severity** Get the values of the configured settings.
- **snmp show** Show the current list of SNMP management servers.
- **snmp exportmib url** Upload the SNMP MIB file to the given URL. The URL supports FTP and SCP. If the URL specifies a remote directory, the default filename is access_mib.txt.

13.6.4 EXAMPLES

Add a new SNMP management server.

```
Report> snmp add mgmtserv1.veritas.com
OK Completed
```

Delete a configured SNMP management server.
Report> snmp delete mgmtserv2.veritas.com
OK Completed

Pass invalid value for SNMP server deletion

Report> snmp delete mgmtserv22.veritas.com
ACCESS snmp delete ERROR V-288-26 Cannot delete SNMP management server, it doesn't exist.

Show the configured SNMP management servers.

Report> snmp show
Configured SNMP management servers:
public@mgmtserv1.veritas.com, public@mgmtserv2.veritas.com
OK Completed

Upload the SNMP MIB file:

Report> snmp exportmib scp://admin@server1.veritas.com:/tmp/access_mib.txt
Password: *****
OK Completed

Set SNMP events filter:

Report> snmp set filter all
OK Completed

Get configured SNMP events filter:

Report> snmp get filter
Filter for the events: all
OK Completed

Set SNMP events severity:

Report> snmp set severity info
OK Completed

Get configured SNMP events severity:

Report> snmp get severity
Severity of the events: info
OK Completed

13.6.5 SEE ALSO

eMail(1), exportevents(1), showevents(1), syslog(1), event(1)
13.7 syslog

13.7.1 SYNOPSIS

syslog add syslog-server-ipaddr
syslog delete syslog-server-ipaddr
syslog set filter|severity value
syslog get filter|severity
syslog show

13.7.2 DESCRIPTION

The report syslog command configures external syslog servers, the filter for the events and the severity of the events. The event notifications matching configured severity and filter are logged to those external syslog servers.

13.7.3 OPTIONS

syslog-server-ipaddr  Hostname or IP address of the external syslog server.
value  Value of the variable to set.
syslog add syslog-server-ipaddr  Add an external syslog server.
syslog delete syslog-server-ipaddr  Delete a syslog server from the configured syslog servers.
syslog set filter value  Set filter for syslog notifications. Events matching with given filter will be sent for notifications.
syslog set severity value  Set severity for syslog notifications. Events having same or higher severity will be sent for notifications.
syslog get filter|severity  Get the values of the configured settings.
syslog show  Show the current list of external syslog servers.

13.7.4 EXAMPLES

Add a new syslog server.

Report> syslog add syslog1.veritas.com

Delete a configured syslog server.

Report> syslog delete syslog2.veritas.com

Show configured syslog servers.

Report> syslog show
Configured syslog servers:
syslog1.veritas.com, syslog2.veritas.com

Set syslog events filter:
**13.7.5 SEE ALSO**

email(1), exportevents(1), snmp(1), showevents(1), event(1)
14.1 replication

14.1.1 SYNOPSIS

config bind ip_addr [device] [netmask]
config unbind ip_addr
config show [ip | remote_clus]
config import_keys [URL]
config export_keys [URL]
config del_keys console_ip
config auth console_ip link_name
config deauth link_name
config check link_name
config certificate generate
config certificate import
config certificate delete
config certificate status
service start [node_name]
service stop
service status
repunit create repunit_name repunit_entry*[,*repunit_entry,...]
repunit add_entry repunit_name repunit_entry
repunit add_pattern_entry repunit_name repunit_pattern_entry
repunit remove_entry repunit_name repunit_entry
repunit remove_pattern_entry repunit_name repunit_pattern_entry
repunit modify_entry repunit_name old_repunit_entry new_repunit_entry
repunit modify_pattern_entry repunit_name old_repunit_pattern_entry new_repunit_pattern_entry
repunit destroy repunit_name [option]
repunit show [repunit_name] | [verbose]
rpo show job_name [duration]
exclunit create exclunit_name exclunit_entry*[,exclunit_entry,...]
exclunit add_entry exclunit_name exclunit_entry
exclunit add_pattern_entry exclunit_name exclunit_pattern_entry
exclunit remove_entry exclunit_name exclunit_entry
exclunit remove_pattern_entry exclunit_name exclunit_pattern_entry
exclunit modify_entry exclunit_name old_exclunit_entry new_exclunit_entry
exclunit modify_pattern_entry exclunit_name old_exclunit_pattern_entry new_exclunit_pattern_entry
exclunit destroy exclunit_name
exclunit show [exclunit_name]
schedule create schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
schedule modify schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
schedule show [schedule_name]
schedule delete schedule_name
job create job_name src_repunit tgt_repunit link_name schedule_name [evpsn]
job show [job_name]
job enable job_name
job sync job_name
job status job_name
job pause job_name
job resume job_name
job disable job_name
job destroy job_name [option]
job abort job_name
job failover force job_name [link_name]
job failback force job_name [link_name]
job exclude job_name exclunit_name
job modify debug job_name on|off
job modify tunables job_name netconn rwcount
bwlimit set link_name limit
bwlimit show [link_name]
sync enable fs_name pool_name link_name
14.1.2 DESCRIPTION

These replication commands are used to manage the replication service on a cluster.

14.1.3 OPTIONS

config bind ip_addr [device] [netmask]
    Add a virtual IP address to be used as the replication service virtual IP address and device as a network interface for the virtual IP address.

config unbind ip_addr
    Delete the virtual IP address from the replication service.

config export_keys URL
    Copy the replication public key from the local cluster to a specified URL.

config import_keys URL
    Copy the replication public key of the remote cluster from a specified URL to a local cluster.

config del_keys console_ip
    Delete the replication public key of a remote cluster identified by console_ip from the local cluster.

config auth console_ip link_name
    Authenticate two clusters mutually to participate in the replication service. The * console_ip * is the console IP address of the remote cluster, and link_name is the association name between the local cluster and the remote cluster.

config deauth link_name
    Unauthenticate two clusters identified by the association link_name from participating in the replication service.

config check link_name
    Check the status of the association identified by the name link_name between the source and the target clusters.

config certificate generate
Generate a self-signed certificate.

```bash
config certificate import
```
Import trusted certificates from an external entity.

```bash
config certificate delete
```
Delete configured certificates.

```bash
config certificate status
```
Display certificate information.

```bash
service start [node_name]
```
Start the replication service. You can use the optional parameter “node_name” to start the replication service on a specific node of the cluster. Otherwise the service start command will automatically figure out the best suitable node in the cluster and will start the replication service there.

```bash
service stop
```
Stop the replication service.

```bash
service status
```
Check the status of the replication service.

```bash
repunit create repunit_name repunit_entry*,*repunit_entry,...]
```
Create a replication unit with a given set of entries.

```bash
repunit add_entry repunit_name repunit_entry
```
Add a new entry to an existing replication unit.

```bash
repunit add_pattern_entry repunit_name repunit_pattern_entry
```
Add a new pattern entry to an existing replication unit.

```bash
repunit remove_entry repunit_name repunit_entry
```
Remove an entry from an existing replication unit.

```bash
repunit remove_pattern_entry repunit_name repunit_pattern_entry
```
Remove a pattern entry from an existing replication unit.

```bash
repunit modify_entry repunit_name old_repunit_entry new_repunit_entry
```
Modify an existing entry in a replication unit.

```bash
repunit modify_pattern_entry repunit_name old_repunit_pattern_entry new_repunit_pattern_entry
```
Modify an existing pattern entry in a replication unit.

```bash
repunit destroy [repunit_name] [option]
```
Destroy a replication unit.

```bash
repunit show [repunit_name] [verbose]
```
Display replication unit details.

```bash
rpo show job_name [duration]
```
Display RPO of the job.

```bash
exclunit create exclunit_name exclunit_entry*,*exclunit_entry,...]
```
Create an excluding unit with a given set of entries.
exclunit add_entry exclunit_name exclunit_entry
   Add a new entry to an existing excluding unit.

exclunit add_pattern_entry exclunit_name exclunit_pattern_entry
   Add a new pattern entry to an existing excluding unit.

exclunit remove_entry exclunit_name exclunit_entry
   Remove an entry from an existing excluding unit.

exclunit remove_pattern_entry exclunit_name exclunit_pattern_entry
   Remove a pattern entry from an existing excluding unit.

exclunit modify_entry exclunit_name old_exclunit_entry new_exclunit_entry
   Modify an existing entry in an excluding unit.

exclunit modify_pattern_entry exclunit_name old_exclunit_pattern_entry new_exclunit_pattern_entry
   Modify an existing pattern entry in an excluding unit.

exclunit destroy exclunit_name
   Destroy an excluding unit.

exclunit show [exclunit_name]
   Display excluding unit details.

schedule create schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
   Create a schedule.

schedule modify schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
   Modify an existing schedule.

schedule show schedule_name
   Show a schedule.

schedule delete schedule_name
   Delete a schedule.

job create job_name src_repunit tgt_repunit link_name schedule_name [evpsn]
   Create a replication job definition.

   evpsn  The evpsn option [evpsn =yes|evpsn=no] enables or disables Enterprise Vault partition secure no-
   tifications.

job show [job_name]
   Display the definition of a job.

job enable job_name
   Activate a job and start replicating the data.

job status [job_name]
   Show status of job(s).

job pause job_name
   Pause an already running job.
job resume job_name
    Resume an already paused job.

job disable job_name
    Disable an Enabled/Paused/Failed job.

job destroy job_name [option]
    Destroy a job. The administrator can use the force option to clean up local jobs. In case of forceful job removal, configuration of the other clusters, which are part of the job, will not be modified and repunit(s) will be disassociated from the job. Job destroy force should be used in case of unrecoverable configuration or replication direction mismatch.

job abort job_name
    Abort an already running job.

job sync job_name
    Start a sync job. This command is similar to the job enable command but will stop the replication job after one iteration (full or incremental) is complete. This command can also be used if the primary file system is completely destroyed and needs to be recovered from the secondary site after a disaster.

job failover force job_name [link_name]
    Failover the job from the source cluster to one of the available target clusters of link link_name. Job failover can be executed from the target with empty link_name when the source cluster is not available. If the failover command executed from the target (when the source is not available), configuration related to the old source will be deleted. The administrator can use the job failover command from this old source with link_name of the new source to configure left-over source as the target of the current new source.

force The force option [force=yes|force=no] gives the option of interactive failover.

job failback force job_name [link_name]
    Failback the job from the source (previous target) cluster to the target (previous source) cluster. link_name is the link to the target cluster.

force The force option [force=yes|force=no] gives the option of interactive failback.

job exclude job_name exclunit_name
    Add an excluding unit to a job.

job modify debug job_name on|off
    Enable or disable debugging for the given job.

job modify tunables job_name netconn rwcount
    Set the tunables (sockets and threads) for the given job.

bwlimit set link_name limit
    Set bandwidth limit for given link.

bwlimit show [link_name]
    Display the bandwidth limit value of the replication links.

sync enable fs_name pool_name link_name:
    Configure the sync replication between the source and the target cluster. It requires fs_name, which should be present on the source cluster, pool_name, which should be present on the target cluster, and link_name, which is created during authentication of the source and the target cluster.
sync disable fs_name link_name:
   Unconfigure sync replication from the source and the target cluster. It requires fs_name and link_name as parameters.

sync migrate fs_name:
   Migrate the roles of primary and secondary in synchronous replication. It requires fs_name as parameter for which primary and secondary roles has to change.

sync start fs_name:
   Start data replication between the source and the target cluster.

sync stop fs_name:
   Stop data replication between the source and the target cluster.

sync pause fs_name:
   Pause data replication between the source and the target cluster.

sync resume fs_name:
   Resume data replication between the source and the target cluster, which was paused.

sync status fs_name:
   Display the status of synchronous replication between the source and the target cluster.

sync failover fs_name:
   Failover the synchronous replication from the source cluster to target cluster. The sync failover can be executed from the target cluster when the source cluster is not available. If the failover command executed from the target (when the source is not available), it will run the application on the target cluster.

sync failback fs_name:
   Failback the synchronous replication from the source (previous target) cluster to the target (previous source) cluster.

sync show
   Show the list of file system which are configured under synchronous replication.

14.1.4 SEE ALSO

config(1), service(1), repunit(1), rpo(1), exclunit(1), bwlimit(1), job(1), sync(1)
14.2 bwlimit

14.2.1 SYNOPSIS

bwlimit set link_names limit
bwlimit reset link_names
bwlimit show [link_names]

14.2.2 DESCRIPTION

The replication bwlimit command allows administrators to set, modify, disable, or display bandwidth allocation limits set for a replication link.

bwlimit set command sets, modifies, disables bandwidth limit on the specified links in the current cluster. This command does not set the bandwidth limit on the counter part of the link. You need to set the limit on each cluster. The bandwidth limit unit is kilobits per second (kbps). Specifying the limit value of 0 disables the bandwidth limit enabled on the specified links.

bwlimit reset command disables the bandwidth limit enabled on the specified links or alternatively, specify limit value as 0 while setting the limit.

bwlimit show command by default displays bandwidth limit information for all the links. To show bandwidth limit set for specific links, use bwlimit show with the link name.

14.2.3 OPTIONS

bwlimit set link_names limit  This command sets/modifies/disables the bandwidth limit for the specified links on the current cluster.

bwlimit reset link_names  This command disables the bandwidth limit for the specified links on the current cluster.

bwlimit show [link_names]  This command displays the configured bandwidth limit values for all or the specified links on the current cluster.

14.2.4 EXAMPLES

The following command sets the bandwidth limit of 50 kbps on the pune_cdc, pune_mtv, and pune_uk links:

Replication>bwlimit set pune_cdc,pune_mtv,pune_uk 50

The following command changes the bandwidth limit on just the pune_cdc link to 20 kbps:

Replication>bwlimit set pune_cdc 20

Either of the following commands disable the bandwidth limit on the pune_uk link:

Replication>bwlimit set pune_uk 0
Replication>bwlimit reset pune_uk

The following command displays the bandwidth limit set for all the replication links:
Replication>bwlimit show

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Bandwidth (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>pune_cdc</td>
<td>20</td>
</tr>
<tr>
<td>pune_mtv</td>
<td>50</td>
</tr>
<tr>
<td>pune_uk</td>
<td>Unlimited</td>
</tr>
</tbody>
</table>

The following command displays the bandwidth limit of only pune_cdc and pune_mtv replication links:

Replication>bwlimit show pune_cdc,pune_mtv

<table>
<thead>
<tr>
<th>Link Name</th>
<th>Bandwidth (kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>pune_cdc</td>
<td>20</td>
</tr>
<tr>
<td>pune_mtv</td>
<td>50</td>
</tr>
</tbody>
</table>

14.2.5 SEE ALSO

config(1)
14.3 config

14.3.1 SYNOPSIS

config bind ip_addr [device] [netmask]
config show [ip | remote_clus]
config unbind ip_addr
config export_keys [URL]
config import_keys [URL]
config del_keys conIP
config auth conIP link_name
config deauth link_name
config check link_name
config certificate generate
config certificate import
config certificate delete
config certificate status

14.3.2 DESCRIPTION

The replication config command provides a set of cluster authentication related operations and methods to add and delete a virtual IP with the replication service.

Veritas Access replication authentication strategy is based on RSA key authentication, and both source and destination clusters have to export their replication public keys. Both the source and destination clusters must then import public keys from each other.

After both the source and destination clusters have successfully imported each other’s keys, the config auth command must be run on the source cluster to complete the authentication between the two clusters. The config auth command will check two-way communication between the source and the destination clusters, and then it will authenticate these two clusters to participate in the replication service.

14.3.3 OPTIONS

config bind ip_addr [device] [netmask] Add a virtual IP address to be used as the replication service virtual IP address and device as a network interface for the virtual IP address. The ip_addr is highly-available in the cluster. By default, the replication virtual IP address is configured on the pubeth0 interface using the pubeth0 interface netmask. You can change the default interface and the netmask using [device] and [netmask] parameters.

config show [ip | remote_clus] Display the replication virtual IP (using the ip option) of the local cluster. remote_clus option of the config show command displays information related to the remote cluster replication VIP as well as information related to key import and authentication status.

config unbind ip_addr Delete the virtual IP address from the replication service.
**config export_keys [URL]** Copy the replication public key from the local cluster to a specified URL.

**config import_keys [URL]** Copy the replication public key of the remote cluster from a specified URL to the local cluster.

**config del_keys conIP** Delete the replication public key of a remote cluster identified by `conIP` from the local cluster.

**config auth conIP link_name** Authenticate two clusters mutually to participate in the replication service. The `conIP` is the console IP address of the remote cluster, and `link_name` is the association name between the local cluster and the remote cluster.

**config deauth link_name** Un-authenticate two clusters identified by the association `link_name` from participating in the replication service.

**config check link_name** Check the status of the association identified by the name `link_name` between the source and the destination clusters.

**config certificate generate** Generate a self-signed certificate.

**config certificate import** Import trusted certificates from an external entity.

**config certificate delete** Delete configured certificates.

**config certificate status** Display certificate information.

### 14.3.4 EXAMPLES

Add a VIP address for the replication service.

```
Replication> config bind 10.209.107.89
Please wait...
Completed
```

Configure VIP address for the replication service on interface pubeth1 and netmask 255.255.248.0.

```
Replication> config bind 10.209.107.89 pubeth1 255.255.248.0
Please wait...
Completed
```

Show the replication VIP address.

```
Replication> config show ip
Replication VIP :: 10.209.107.89
```

Delete the replication VIP from the replication service.

```
Replication> config unbind 10.209.107.89
Please wait...
Completed
```

Export replication key of the local cluster to the home directory of fBssnasfp user at URL `ssnasweb.vxindia.veritas.com`.

```
Replication> config export_keys scp://ssnas@ssnasweb.vxindia.veritas.com:~/
Password: ******
ACCESS Replication SUCCESS V-288-0 Key file ISAKEY_source_10.209.105.128_2009-05-29 copied successfully at location ssnasweb.vxindia.veritas.com:~/
```
Import key of a remote cluster from the home directory of `ssnas user` at URL `ssnasweb.vxindia.veritas.com`.

```bash
Replication> config import_keys scp://ssnas@ssnasweb.vxindia.veritas.com:~/ISAKEY_˓→source_10.209.105.236_2009-05-29
Password: *****
```

Show list of cluster(s) whose key is imported by the local cluster.

```bash
Replication> config show remote_clus
Link name   Remote cluster ConsoleIP   Remote cluster Replication IP   Time of Key_˓→Import   Time of Authorization
--------------   ---------------------   ---------------------   ---------------------   ---------------------   ---------------------
---           ---           ---           ---           ---           ---
```

Authorize a remote cluster having console IP 10.209.105.236 and link name as Pune_Shanghai.

```bash
Replication> config auth 10.209.105.236 Pune_Shanghai
```

Show list of authorized clusters.

```bash
Replication> config show remote_clus
Link name   Remote cluster ConsoleIP   Remote cluster Replication IP   Time of Key_˓→Import   Time of Authorization
--------------   ---------------------   ---------------------   ---------------------   ---------------------   ---------------------
---           ---           ---           ---           ---           ---
```

### 14.3.5 SEE ALSO

`service(1), job(1)`
14.4 exclunit

14.4.1 SYNOPSIS

exclunit create exclunit_name exclunit_entry [, exclunit_entry,...]
exclunit add_entry exclunit_name exclunit_entry
exclunit remove_entry exclunit_name exclunit_entry
exclunit modify_entry exclunit_name old_exclunit_entry new_exclunit_entry
exclunit destroy exclunit_name
exclunit show [exclunit_name]

14.4.2 DESCRIPTION

The replication exclunit command provides operations to create, destroy, show, and manage excluding unit definitions.

An excluding unit is a collection of files that you do not want to replicate. Hence, all files belonging to an excluding unit are not replicated from the source cluster to the destination cluster.

A single excluding unit can span across multiple directories and is common for all file systems. An excluding unit is defined as an ordered set of entries, where each entry is one of the following:

- Directory
- Single file

The entry is identified by the path of the directory, or the file. The entry should be the substring following the file system root. For example, /vx/fs1/dir1/file specifies dir1/file as the exclunit entry. Member entries are ordered inside an excluding unit.

The exclunit entry has higher priority over the repunit entry. If any existing file name matches the exclunit entry, the file/directory is not replicated to the target.

14.4.3 OPTIONS

exclunit create exclunit_name exclunit_entry [, exclunit_entry,...] Create an excluding unit with a given set of entries.
exclunit add_entry exclunit_name exclunit_entry Add a new entry to an existing excluding unit.
exclunit remove_entry exclunit_name exclunit_entry Remove an entry from an existing excluding unit.
exclunit modify_entry exclunit_name old_exclunit_entry new_exclunit_entry Modify an existing entry in a excluding unit.
exclunit destroy exclunit_name Destroy an excluding unit.
exclunit show [exclunit_name] Display excluding unit details.
14.4.4 EXAMPLES

Create an excluding unit exclu1 with entries DB_CONFIG, SQL_CONFIG, and DB_DIR/conf_file.

```bash
Replication> exclunit create exclu1 DB_CONFIG,SQL_CONFIG,DB_DIR/conf_file
ACCESS Replication SUCCESS V-288-0 Excluding unit exclu1 created successfully.
```

Display the definition of the exclunit exclu1.

```bash
Replication> exclunit show exclu1
exclunit name: exclu1
======================
fs name: 
--------
paths: 
------
DB_CONFIG
SQL_CONFIG
DB_DIR/conf_file
patterns: 
---------
jobs: 
-----
new_job1
```

Add an entry DB_DIR/new_conf_file in the excluding unit definition exclu1.

```bash
Replication> exclunit add_entry exclu1 DB_DIR/new_conf_file
```

Delete an entry DB_DIR/new_conf_file from the excluding unit definition exclu1.

```bash
Replication> exclunit remove_entry exclu1 DB_DIR/new_conf_file
```

Modify an entry DB_DIR/new_conf_FILE to DB_DIR/new_conf_FILE_1 in the excluding unit definition exclu1.

```bash
Replication> exclunit modify_entry exclu1 DB_DIR/new_conf_file DB_DIR/new_conf_file_1
```

14.4.5 SEE ALSO

job(1), config(1), schedule(1)
14.5 job

14.5.1 SYNOPSIS

job create job_name src_repunit tgt_repunit link_name schedule_name [evpsn]
job show [job_name]
job enable job_name
job sync job_name
job status [job_name]
job pause job_name
job resume job_name
job disable job_name
job destroy job_name [option]
job abort job_name
job failover force=yes/no job_name [link_name]
job failback force=yes/no job_name link_name
job exclude job_name exclunit_name
job modify debug job_name on|off
job modify tunables job_name netconn rwcount

14.5.2 DESCRIPTION

The replication job command provides operations to create, destroy, display, and manage job definitions and job states.

A job binds together source and target replication units, the source and the target clusters, and a replication schedule. A configured job defines who participates in replication, what gets replicated, and when replication occurs between the source and the target clusters.

14.5.3 OPTIONS

job create job_name src_repunit tgt_repunit link_name schedule_name [evpsn]

Create a replication job with source replication unit, target replication unit and the link name.

The evpsn option [evpsn =yes|evpsn=no] option enables or disables Enterprise Vault partition secure notifications.

job show [job_name]

Display the definition of a job.

job enable job_name

Start a job and add it to the replication scheduler queue. The actual replication of data starts on the next schedule of the job.

job status [job_name]
Display status of job(s).

`job pause job_name`

Pause a running job.

`job resume job_name`

Resume a paused job.

`job disable job_name`

Disable an enabled job.

`job destroy job_name [option]`

**Destroy a job.** The administrator can use the force option to clean up the local job. In case of forceful job removal, configuration of the other clusters, which are part of the job, are not modified and repunit(s) are disassociated from the job. Job destroy force should be used in case of unrecoverable configuration or replication direction mismatch.

`job abort job_name`

Abort a running job.

`job sync job_name`

This command is similar to the job enable command but will stop the replication job after one iteration (full or incremental) is complete. This command can also be used if the primary file system is completely destroyed and needs to be recovered from the secondary site after a disaster.

`job failover force job_name [link_name]`

**Failover the job from the source cluster to one of the available target clusters of link link_name.**

Job failover can be executed from the target with empty `link_name` when the source cluster is not available. If the failover command executed from the target (when the source is not available), configuration related to the old source is deleted. The administrator can use the job failover command from this old source with the `link_name` of the new source to configure the leftover source as the target of the current new source.

`job failback force job_name link_name`

Failback the job from the source (previous target) cluster to the target (previous source) cluster. `link_name` is the link to the target cluster.

`job exclude job_name exclunit_name`

Add excluding unit to a specified job. `exclunit_name` is the excluding unit name to add for job `job_name`.

`job modify debug job_name on|off`

Enable or disable debugging for the given job.

`job modify tunables job_name netconn rwcount`

Set the tunables (sockets and threads) for the given job.

### 14.5.4 EXAMPLES

Create a job with name `new_job1`, source replication unit `srp1`, target replication unit `trp1`, link name as `Pune_Shanghai`, and schedule as `s1`.

```
Replication> job create new_job1 srp1 trp1 Pune_Shanghai s1
Completed successfully.
```
Display definition of job `new_job1`:

```
Replication> job show new_job1

<table>
<thead>
<tr>
<th>Job Name</th>
<th>Role</th>
<th>Debug</th>
<th>Schedule</th>
<th>State</th>
<th>Exclunit</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>new_job1</td>
<td>SOURCE</td>
<td>ON</td>
<td>sch1</td>
<td>ENABLED</td>
<td>--</td>
<td>srp1</td>
</tr>
</tbody>
</table>
```

Check status of a job `new_job1`:

```
Replication> job status new_job1
Job 'new_job1' configured but not running.
```

Enable a job `new_job1`:

```
Replication> job enable new_job1
```

Pause a running job `new_job1`:

```
Replication> job pause new_job1
```

Resume a paused job `new_job1`:

```
Replication> job resume new_job1
```

Disable an enabled job `new_job1`:

```
Replication> job disable new_job1
```

Destroy a disabled job `new_job1`:

```
Replication> job destroy new_job1
```

Abort a running job `new_job1`:

```
Replication> job abort new_job1
```

Start sync on a disabled job `new_job1`:

```
Replication> job sync new_job1
```

Failover the job `new_job1` corresponding to the link `Pune_Shanghai` to target cluster. In planned failover scenarios, the administrator can use this command.

```
Replication> job failover force=no new_job1 Pune_Shanghai
```

Failback the job `new_job1` to the source cluster from the target cluster.

```
Replication> job failback force=no new_job1 Pune_Shanghai
```

Add excluding unit `exclu1` to job `new_job1`:

```
Replication> job exclude new_job1 exclu1
```

Modify the job with tunables.

---

14.5. `job`
14.5.5 SEE ALSO

config(1), repunit(1), schedule(1), exclunit(1)
14.6 repunit

14.6.1 SYNOPSIS

repunit create repunit_name repunit_entry[/,repunit_entry,...]
repunit add_entry repunit_name repunit_entry
repunit remove_entry repunit_name repunit_entry
repunit modify_entry repunit_name old_repunit_entry new_repunit_entry
repunit destroy repunit_name [option]
repunit show [repunit_name] | [verbose]

14.6.2 DESCRIPTION

The replication repunit command provides operations to create, destroy, show, and manage replication unit definitions. A replication unit is a collection of files that you want to include in a replication job. All files belonging to a replication unit are replicated together from the source cluster to the target cluster.

A single replication unit can span across multiple directories and even multiple file systems. A replication unit is defined as an ordered set of entries, where each entry is one of the following:

- File system
- Subdirectory
- Single file

The entry is identified by the file system name optionally followed by a slash ('/'), followed by the path of the directory, or the file inside the file system. Member entries are ordered inside a replication unit and such ordering information is used for the mapping between the source and the target replication units.

The user can specify a file/directory name to replicate files based on file name, which will select files dynamically. The user does not need to know the exact file name in advance.

The exclunit entry have higher priority over the repunit entry. If any path name matches the exclunit entry or the exclunit the file/directory is not replicated to the target. Also, if any path matches both the repunit and the exclunit, the path is not replicated to the target. Based on dataset known, the user can specify either the repunit or the exclunit.

14.6.3 OPTIONS

repunit create repunit_name repunit_entry [, repunit_entry,...] Create a replication unit with a given set of entries.
repunit add_entry repunit_name repunit_entry Add a new entry to an existing replication unit.
repunit remove_entry repunit_name repunit_entry Remove an entry from an existing replication unit.
repunit modify_entry repunit_name old_repunit_entry new_repunit_entry Modify an existing entry in a replication unit.
repunit destroy repunit_name [option] Destroy a replication unit. With force option, repunit is removed even if the associated job exists.
repunit show [repunit_name] | [verbose] Display replication unit details.
Display compact list if no option is provided.
Use ‘verbose’ keyword to display all repunit details including paths.

### 14.6.4 EXAMPLES

Create a replication unit ru1 with entries fs1/DB_CONFIG, fs1/SQL_CONFIG and fs1/conf_file.

```
Replication> repunit create ru1 fs1/DB_CONFIG,fs1/SQL_CONFIG,fs1/conf_file
```

Display the definition of a repunit ru1.

```
Replication> repunit show ru1
repunit name: ru1
fs name: ---------
fs1,fs2
paths: -------
fs1/DB_CONFIG
fs1/SQL_CONFIG
fs1/conf_file
fs2/conf_file
patterns: ---------
jobs: -------
new_job1
```

Add an entry fs1/new_conf_file in the replication unit definition ru1.

```
Replication> repunit add_entry ru1 fs1/new_conf_file,fs2/new_config_dir1
```

Delete an entry fs1/new_conf_file from the replication unit definition ru1.

```
Replication> repunit remove_entry ru1 fs1/new_conf_file
```

Modify an entry fs1/new_conf_file to fs1/new_conf_file_1 in the replication unit definition ru1.

```
Replication> repunit modify_entry ru1 fs1/new_conf_file fs1/new_conf_file_1
```

### NOTES

Removing the repunit entry does not remove the file system from the repunit, even when the entry is the last entry for the file system. The next replication cycle tries to replicate complete “/” for that file system.

### 14.6.5 SEE ALSO

job(1), config(1), schedule(1)
14.7 rpo

14.7.1 SYNOPSIS

rpo show job_name [duration]

14.7.2 DESCRIPTION

rpo show command shows the current RPO of the given job and also shows the average RPO times over the last 24 hours, the last week, and the last month. The optional parameter duration can be used to show the average RPO over the last given number of hours.

14.7.3 EXAMPLES

Show current RPO, average RPO times over the last 24 hours, the last week, and the last month of the job job1.
In the below example, the current RPO is 20 minutes 17 seconds, in the last 24 hours, the average RPO is 1 hour 5 minutes 20 seconds. Last week’s average RPO is 30 minutes 10 seconds, the last 1 month average RPO is 45 minutes 40 seconds.

<table>
<thead>
<tr>
<th>JOB NAME</th>
<th>CURRENT RPO</th>
<th>LAST 24 AVG RPO</th>
<th>LAST 1 WEEK AVG RPO</th>
<th>LAST 1 MONTH AVG RPO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job1</td>
<td>20:17 Seconds</td>
<td>1:05:20 Seconds</td>
<td>30:10 Seconds</td>
<td>45:40 Seconds</td>
</tr>
</tbody>
</table>

Show the average RPO over the last 5 hours of the job job1. Duration range is 1 hour to 720 hours. In the below example, the average RPO over the last 5 hours is 30 minutes 35 seconds.

Replication>rpo show job1 5
ACCESS replication INFO V-288-1590 Avg RPO from last 5 hr: 30:35 Seconds

14.7.4 SEE ALSO

job(1)
14.8 schedule

14.8.1 SYNOPSIS

```
schedule create schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
schedule modify schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
schedule show [schedule_name]
schedule delete schedule_name
```

14.8.2 DESCRIPTION

The replication schedule commands create, destroy, display, and manage the replication schedules.

Veritas Access supports periodic replication, where the data gets replicated from the source to the destination at regular intervals as defined by the schedule. The same schedule definition can be used for multiple replication jobs. The input to create a schedule is in the same format as that required by the standard UNIX cron daemon, where the values for minute, hour, day-of-the-month, month, and day-of-the-week, are almost the same as the crontab format. The parameters and values are defined below.

1. **Schedule name:** Specifies the name of the schedule.
2. **Minute:** This parameter contains either an asterisk `*`, which implies run every minute, or a numeric value between the range of 0-59.
3. **Hour:** This parameter contains either an asterisk `*`, which implies run every hour, or a numeric value between the range of 0-23.
4. **Day of month:** This parameter contains either an asterisk `*`, which implies run every day of the month, or a numeric value between the range of 1-31.
5. **Month:** This parameter contains either an asterisk `*`, which implies run every month, or a numeric value between the range of 1-12. In addition, this field accepts names of the month. Enter the first three letters of the month (not case-sensitive) as the input value.
6. **Day of Week:** This parameter contains either an asterisk `*`, which implies run every day of the week, or a numeric value between the range of 0-6, with 0 interpreted as Sunday. In addition, this field accepts names of the week. Enter the first three letters of the month (only use lowercase letters) as the input value.

**NOTES:**

1. By default, the optional arguments hour, day-of-the-month, month, and day-of-the-week for the schedule create command contain an asterisk `*`. The minute parameter is a mandatory argument for the schedule create and modify commands.
2. The parameters minute, hour, day-of-the-month, month, and day-of-the-week for schedule create and schedule modify can accept numeric values in the form of ranges, where a range is defined as two numbers separated by a hyphen. To run the schedule between 1 a.m. and 4 a.m., specify the inclusive range 1-4 for the hour parameter.
3. In addition, the parameters can also accept a set of numbers separated by a comma. For example: ‘1,3,5,7’, or ‘1-4’, ‘5-10’.
14.8.3 OPTIONS

```
schedule create schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
Create a schedule.

schedule modify schedule_name minute [hour] [day_of_the_month] [month] [day_of_the_week]
Modify an existing schedule.

schedule show [schedule_name]  Display a schedule.

schedule delete schedule_name  Delete a schedule.
```

14.8.4 EXAMPLES

Create a schedule `s1` to run a job every 30 minutes.

```
Replication> schedule create s1 */30
```

Display schedule `s1`.

```
Replication> schedule show s1
Schedule Name  Minute  Hour  Day  Month  WeekDay
-------------  ------  -----  -----  ------  --------
s1            */30   *     *     *     *
```

Modify a schedule `s1` to run a job every 40 minutes.

```
Replication> schedule modify s1 40
```

Delete a schedule `s1`.

```
Replication> schedule delete s1
```

14.8.5 SEE ALSO

repunit (1), job(1), config(1)
14.9 service

14.9.1 SYNOPSIS

service start [node_name]
service stop
service status

14.9.2 DESCRIPTION

The replication service commands start, stop, and display the status of the replication service. Before starting the Veritas Access Replication service, make sure that:

1. A file system is present on the cluster.
2. A virtual IP address is added to the replication service. Refer to the replication_config.1 man page for more information.

14.9.3 OPTIONS

service start [node_name] Start the replication service. You can use the optional parameter “node_name” to start the replication service on a specific node of the cluster. Otherwise the service start command automatically figures out the best suitable node in the cluster and starts the replication service there.

service stop Stop the replication service.

service status Check the status of the replication service.

14.9.4 EXAMPLES

Start the replication service.

Replication> service start

Check the status of the replication service.

Replication> service status
Replication service RUNNING on node nasg01_01.

Stop the replication service.

Replication> service stop

14.9.5 SEE ALSO

config(1), job(1)
14.10 sync

14.10.1 SYNOPSIS

sync config bind ip_addr [device] [netmask]
sync config show [ip | remote_clus]
sync config unbind ip_addr
sync config export_keys [URL]
sync config import_keys [URL]
sync config del_keys conIP
sync config auth conIP link_name
sync config deauth link_name
sync service start [node_name]
sync service stop
sync service status
sync enable fs_name pool_name link_name
sync disable fs_name link_name
sync start fs_name
sync stop fs_name
sync pause fs_name
sync resume fs_name
sync status fs_name
sync failover fs_name
sync failback fs_name
sync show
sync migrate fs_name

14.10.2 DESCRIPTION

The replication sync command provides synchronous replication between the source and the target cluster, which is based on volume-level replication.

Synchronous replication replicates the application writes on the file system at the source location to one remote location across any distance. It provides a consistent copy of application data at the remote location. If a disaster occurs at the source location, you can use the copy of the application data at the remote location and restart the application at the remote location.
14.10.3 OPTIONS

sync config bind ip_addr [device] [netmask]  Add a virtual IP address which is used as the sync replication service virtual IP address and a device which is used as a network interface for the virtual IP address. The ip_addr is highly-available in the cluster. By default, the replication virtual IP address is configured on the pubeth0 interface using the pubeth0 interface netmask. You can change the default interface and the netmask using the [device] and the [netmask] parameters.

sync config show [ip | remote_clus]  Display the replication virtual IP (using the ip option) of the local cluster. The remote_clus option of the sync config show command displays information related to the remote cluster replication VIP as well as information related to key import and authentication status.

sync config unbind ip_addr  Delete the virtual IP address from the sync replication service.

current config export_keys [URL]  Copy the sync replication public key from the local cluster.

current config import_keys [URL]  Copy the sync replication public key from the remote cluster to the local cluster.

current config del_keys conIP  Delete the sync replication public key of a remote cluster identified by conIP from the local cluster.

current config auth conIP link_name  Authenticate two clusters mutually to participate in the sync replication service. The conIP is the console IP address of the remote cluster, and link_name is the association name between the local cluster and the remote cluster.

current config deauth link_name  Un-authenticate two clusters identified by the association link_name from participating in the sync replication service.

current service start [node_name]  Start the sync replication service. You can use the optional parameter “node_name” to start the replication service on a specific node of the cluster. Otherwise the service start command automatically figures out the best suitable node in the cluster and starts the replication service there.

current service stop  Stop the sync replication service.

sync service status  Check the status of the sync replication service.

sync enable fs_name pool_name link_name  Configure the sync replication between the source and the target cluster. It requires fs_name, which should be present on the source cluster, pool_name, which should be present on the target cluster, and link_name, which is created during authentication of the source and the target cluster. It requires the pool on the target cluster to have sufficient storage to create a file system and Storage Replicated Log (SRL) volume. The SRL volume size is one-fourth of the file system size. For example, if the file system size on the source cluster is 8GB then at least 3GB storage should be present in the pool at the source cluster to create SRL volume. For the target cluster, 11GB storage should be present in pool to create file system and SRL volume.

current disable fs_name link_name  Unconfigure sync replication from the source and the target cluster. It requires fs_name and link_name as parameters.

current start fs_name  Start data replication between the source and the target cluster.

current stop fs_name  Stop data replication between the source and the target cluster.

current pause fs_name  Pause data replication between the source and the target cluster.

sync resume fs_name  Resume data replication between the source and the target cluster, which was paused.

current status fs_name  Display the status of synchronous replication between the source and the target cluster.
**sync failover fs_name** Failover the synchronous replication from the source cluster to target cluster. The sync failover can be executed from the target cluster when the source cluster is not available. If the failover command executed from the target (when the source is not available), it will run the application on the target cluster.

**sync failback fs_name** Failback the synchronous replication from the source (previous target) cluster to the target (previous source) cluster. When the source cluster becomes available, execute failback command from the source cluster to make it new target cluster.

**sync show** Show the list of file system which are configured under synchronous replication.

**sync migrate fs_name** Migrate the roles of primary and secondary in synchronous replication. It requires fs_name as parameter for which primary and secondary roles has to change. This command should be executed from the source cluster.

### 14.10.4 EXAMPLES

Add a VIP address for the replication service.

```
Replication> sync config bind 192.168.10.56
Please wait...
ACCESS replication SUCCESS V-288-0 192.168.10.56 configured as Virtual IP.
ACCESS replication SUCCESS V-288-0 IP bind completed
```

Configure a VIP address for the replication service on interface pubeth1 and netmask 255.255.255.0.

```
Replication> sync config bind 192.168.10.56 pubeth1 255.255.255.0
Please wait...
ACCESS replication SUCCESS V-288-0 192.168.10.56 configured as Virtual IP.
ACCESS replication SUCCESS V-288-0 IP bind completed
```

Show the replication VIP address.

```
Replication> sync config show ip
Local cluster details:
======================
Sync Replication VIP : 192.168.10.56
Online On Node : isaA_01
```

Delete the replication VIP from the replication service.

```
Replication> sync config unbind 192.168.10.57
Please wait...
ACCESS replication SUCCESS V-288-0 IP unbind completed.
```

Export the replication key of the local cluster to the remote cluster.

```
Replication> sync config export_keys
ACCESS replication SUCCESS V-288-1559 Displaying replication key. Please use this key with config import_keys command.
```

```
ssh-rsa AAAAB3NzaC1yc2EAAAABSwAAAAEAtI4Sy9CN7GM0ppfL4NH+bit0/RBoSmYadmLe1D56li1l://
   ClvYJ28ouC5uuYAx/XnCwCFBBGL/uL3+Sqd5+D8+YaRE0cdJvXJEQ2rwU2Ffm+172X1/
   uAbhnrRCS8hvuYm25FgwpYN+6ssDfTDJkse4M3iRCSKASbAS9fh/
   8guCw9yUt1DU1jHlItfTATHEEFk8mesNpq8nOxP88vPPAvNde7BCvWAUERxZQe7CSW5lODT06ft0aFR0hBps8jq261hRz/
   XJuYx3kqiH7cYyj9x/Rmd21U9v== root@isaA_01::isaA_192.168.10.21
```
ACCESS replication SUCCESS V-288-0 Config export keys command completed successfully.

**Import the key of a remote cluster.**

```
Replication> sync config import_keys
Enter replication key of remote cluster::ssh-rsa
AAAAB3NzaC1yc2EAAAABIAwAAAAEQA...root@isaB_02::isaB_192.168.10.22
```

```
Enter console IP address of remote cluster::192.168.10.22
ACCESS replication SUCCESS V-288-0 Config import keys command completed successfully.
```

**Delete the key of a remote cluster.**

```
Replication> sync config del_keys 192.168.10.21
ACCESS replication SUCCESS V-288-0 Config delete keys command completed successfully.
```

**Show the list of cluster(s) whose key is imported by the local cluster.**

```
Replication> sync config show
<table>
<thead>
<tr>
<th>Link name</th>
<th>Remote Console IP</th>
<th>Remote Replication VIP</th>
<th>Time of Key Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>rep1</td>
<td>192.168.10.22</td>
<td>192.168.10.57</td>
<td>Thu May 25 13:31:55 EDT</td>
</tr>
</tbody>
</table>
```

**Authorize a remote cluster having console IP 192.168.10.22 and link name as rep1.**

```
Replication> sync config auth 192.168.10.22 repl
Please wait...
ACCESS replication SUCCESS V-288-0 Config auth command completed successfully.
```

**Unauthorise a remote cluster having link name as rep1.**

```
Replication> sync config deauth repl
Please wait...
ACCESS replication SUCCESS V-288-0 Config deauth command completed successfully.
```

**Show the list of authorized clusters.**

```
Replication> sync config show
<table>
<thead>
<tr>
<th>Link name</th>
<th>Remote Console IP</th>
<th>Remote Replication VIP</th>
<th>Time of Key Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>repl1</td>
<td>192.168.10.22</td>
<td>192.168.10.57</td>
<td>Thu May 25 13:31:55 EDT</td>
</tr>
</tbody>
</table>
```

234 Chapter 14. Replication Commands
Start the replication service.

```
Replication> sync service start
Starting replication service on isaA_01. Please wait...
ACCESS replication SUCCESS V-288-0 Sync Replication service started
```

Stop the replication service.

```
Replication> sync service stop
ACCESS replication SUCCESS V-288-0 Replication service stopped
```

Check the status of the replication service.

```
Replication> sync service status
Status : RUNNING
Online On Node : isaB_01 isaB_02
```

Enable sync replication.

```
Replication> sync enable fs1 pool1 rep1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication configured successfully
```

Disable sync replication.

```
Replication> sync disable fs1 rep1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication unconfigured successfully
```

Start synchronous data replication.

```
Replication> sync start fs1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication service started successfully
```

Stop synchronous data replication.

```
Replication> sync stop fs1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication service stopped successfully
```

Pause synchronous data replication.

```
Replication> sync pause fs1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication service paused successfully
```

Resume synchronous data replication.

```
Replication> sync resume fs1
ACCESS Sync_rep SUCCESS V-288-0 Sync replication service resumed successfully
```

Display the status of synchronous data replication.

```
Replication> sync status fs1
Name value
============================= ================
Replicated Data Set rvg_fs1
Primary Site Info:
Host name 192.168.10.56
RVG state enabled for I/O
```
Failover the synchronous replication corresponding to the fs_name. In unplanned failover scenarios, the administrator can use this command.

```
Replication> sync failover sync_fs
ACCESS Sync_rep SUCCESS V-288-0 Secondary has become new primary. Failover operation executed successfully!
```

Failback the synchronous replication.

```
Replication> sync failback sync_fs
ACCESS Sync_rep SUCCESS V-288-0 Original primary has become secondary. Failback operation executed successfully!
```

Show the list of file system which are configured under synchronous replication.

```
Replication> sync show
sync_fs
```

Migrate the roles of primary and secondary in synchronous replication.

```
Replication> sync migrate myfs
ACCESS Sync_rep SUCCESS V-288-0 Primary and secondary roles migrated successfully!
```

### 14.10.5 SEE ALSO

config(1), service(1)
15

SmartIO Commands

15.1 SmartIO

15.1.1 SYNOPSIS

cache create node_name disk size fstype cachename
cache delete node_name cache_name
cache grow cache_size node_name cache_name
cache list
cache offline node_name cache_name
cache online node_name cache_name
cache shrink cache_size node_name cache_name
cache stat node_name
device list node_name
fs cachemode {nocache|read|writeback} fs_name
fs disable fs_name
fs enable fs_name
fs flush fs_name
fs list fs_name
fs purge fs_name
fs stat fs_name
file cachemode {nocache|read|writeback} filename
file list filename
file load filename
file pin filename
file restore_access filename
file unpin filename

### 15.1.2 DESCRIPTION

These SmartIO commands are used to create and manage SmartIO Cache. Veritas Access supports read caching on solid-state drives (SSDs) for applications running on Veritas Access file systems. In this scenario, application reads are satisfied from the cache whenever possible. As the application accesses the file system, the file system loads data from the disk into the cache. Application writes go to the disk in the usual way. With each write, the file system synchronizes the cache to ensure that applications never see stale data. If a cache device fails, a file that is cached in read mode is completely present on the disk. Therefore, the cache failure does not affect the application I/Os for the file and the application I/Os continue without interruption. By default, the cache area is enabled for caching. All file systems on the system are cached unless you explicitly disable caching for that file system. You do not need to explicitly enable caching on a file system.

These commands allow creating SmartIO cache, setting cache policies for the file systems files and view the SmartIO cache statistics. The supported SmartIO cache policies are read, writeback, and nocache. These commands also allow you to pin and unpin files and directories to the SmartIO cache. When a policy is set for a directory, all the files under the directory inherit the cache policy. The SmartIO cache is local to the node where it is created. Make sure that you create the SmartIO cache on each node of the Veritas Access cluster.

SmartIO provides write caching in the writeback mode also. In writeback mode, an application write returns success after the data is written to the SmartIO cache, which is usually on an SSD. At a later time, SmartIO flushes the cache, which writes the dirty data to the disk. Writeback caching expects to improve the latencies of synchronous user data writes. Writeback caching is superset of read caching. When writeback caching is enabled, read caching is implicitly enabled. Reads are satisfied from the cache if possible, and the file system transparently loads file data into the cache. Both read and writeback caching may be enabled for the same file at the same time. The writeback caching mode gives good performance for writes, but also means that the disk copy may not always be up to date. If a cache device fails, a file that is cached in writeback mode may not be completely present on the disk. SmartIO has a mechanism to flush the data from the cache device when the device comes back online. The writeback cache policy is supported on a two-node Veritas Access clusters only. Veritas Access supports multiple cache creations.

### 15.1.3 OPTIONS

- `cache create node_name disk size fstype cachename` Create the SmartIO cache on the `cache_name` using the specified SSD disk.
- `cache delete node_name cache_name` Delete the specified SmartIO cache on the the specified node.
- `cache grow cache_size node_name cache_name` Grow the specified SmartIO cache on the specified node. The `cache_size` is specified in GB or TB.
- `cache list` List the SmartIO cache properties on the specified node.
- `cache offline node_name cache_name` Bring the SmartIO cache offline on the specified node.
- `cache online node_name cache_name` Bring the SmartIO cache online on the specified node.
- `cache shrink cache_size node_name cache_name` Shrink the SmartIO cache on the specified node. The `cache_size` is specified in GB or TB.
- `cache stat node_name` Display the SmartIO cache statistics on the specified node.
- `device list node_name` List the SSD devices available on `node_name`.
- `fs cachemode {nocache | read | writeback} fs_name` Set `read`, `nocache` or `writeback` SmartIO cache policy for `fs_name` file system.
**fs disable fs_name** Disable SmartIO cache for the `fs_name` file system. This action stops SmartIO cache for the file system specified.

**fs enable fs_name** Enable SmartIO cache for the `fs_name` file system. This action starts caching for the specified file system.

**fs flush fs_name** Flush the writeback data for the `fs_name` file system. For this command to work, the file system must be configured with writeback cache.

**fs list fs_name** Display the SmartIO cache properties and usage for the `fs_name` file system.

**fs purge fs_name** Purge or remove the cached contents for the `fs_name` file system in SmartIO cache.

**fs stat fs_name** Display detailed SmartIO cache statistics for the `fs_name` file system specified.

**file cachemode {nocache|read|writeback} file_name** Set caching mode for the named file or directory. The supported caching modes are read, nocache or writeback. For directories, caching mode is set recursively.

**file load file_name** Load the named file or directory into the SmartIO cache. The file is loaded asynchronously in the background.

**file pin file_name** Pin the named file or directory into SmartIO cache. The pinned file blocks in the cache generally will not be aged out of the cache.

**file list file_name** List the SmartIO cache properties for the specified `file_name`.

**file restore_access file_name** Enables access to files that are missing writeback data. If the writeback cache data could not be flushed to the disk for some files due to an error, SmartIO prevents access to the files. This command only restores access to the files, but it does not restore the missing data.

**file unpin file_name** Unpin the named file or directory into smartIO cache.

### 15.1.4 EXAMPLES

Create a SmartIO cache.

```
test1.SmartIO> cache create sdb,sdc 2G reserve cache6
SmartIO cache area created
```

List SmartIO cache properties.

```
test1.SmartIO> cache list

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>SIZE</th>
<th>ASSOC-TYPE</th>
<th>STATE</th>
<th>FSTYPE</th>
<th>DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache4</td>
<td>VxFS</td>
<td>2.00g</td>
<td>AUTO</td>
<td>OFFLINE</td>
<td>default</td>
<td>sdb</td>
</tr>
<tr>
<td>cache6</td>
<td>VxFS</td>
<td>2.00g</td>
<td>AUTO</td>
<td>ONLINE</td>
<td>reserve</td>
<td>sdb,sdc</td>
</tr>
</tbody>
</table>
```

Bring the SmartIO cache online.

```
test1.SmartIO> cache online test1_01 cache2
SmartIO cache is online
```

Grow the SmartIO cache.

```
test1.SmartIO> cache grow 16g test1_01 sdd cache2
Smartio cache grow completed
```
Change the fstype of SmartIO cache.

```
test1.SmartIO> cache settype clusA_01 cache5 reserve
ACCESS smartio SUCCESS V-288-999 SmartIO cache fstype change
```

Display SmartIO cache statistics.

```
test1.SmartIO> cache stat

TYPE: VxFS
NAME: sfcachearea_1
  Cache Size: 15.97 GB
  Cache Utilization: 118.0 MB ( 0.72 %)
File Systems Using Cache: 7
Writeback Cache Use Limit: Unlimited
  Writeback Flush Timelag: 10 s

Read Cache          Writeback
Hit Ratio      Data Read      Data Written      Hit Ratio      Data Written

Total:
  8.97 % 52 KB 1 MB 0.00 % 0 KB
/shared:
  8.97 % 52 KB 1 MB 0.00 % 0 KB
```

Set nocache SmartIO policy for file system where TPCC database archivelog files are stored.

```
SmartIO> fs cachemode nocache tpcc_arch1
Cluster-configuration updated with changed Mount Options for node test_01
Mount Point /vx/tpcc_arch1 remounted successfully on test_01
Cluster-configuration updated with changed Mount Options for node test_02
Mount Point /vx/tpcc_arch1 remounted successfully on test_02
```

Enable SmartIO cache for file system where TPCC datafiles are stored.

```
SmartIO> fs enable tpcc_data1
```

List SmartIO cache for file system tpcc_data1

```
SmartIO> fs list tpcc_data1
/vx/tpcc_data1:
  READ CACHE WRITEBACK MODE PINNED NAME
      648 KB     0 KB   read   no /vx/tpcc_data1/cntrlSLOB.ctl
      0 KB     0 KB   read   no /vx/tpcc_data1/SLOB
      648 KB     0 KB   read   no /vx/tpcc_data1
```

List SmartIO cache for file system tpcc_data1

```
SmartIO> fs stat tpcc_data1

  Cache Size:  15.97 GB
  Cache Utilization:  652 KB ( 0.00 %)
  Read Cache
```
### Load system.dbf file into SmartIO cache

```
SmartIO> file load /vx/tpcc_data/system.dbf
SUCCESS: SmartIO cache load for /vx/tpcc_data1/system.dbf on host ISAGA_01
```

### Pin system.dbf file into SmartIO cache

```
SmartIO> file pin /vx/tpcc_data/system.dbf
SUCCESS : SmartIO cache pin for /vx/tpcc_data1/system.dbf
```

### Display SmartIO information for file system.dbf

```
SmartIO> file list /vx/tpcc_data/system.dbf
/vx/tpcc_data1/system.dbf:
READ CACHE WRITEBACK MODE PINNED
16.68 MB 0 KB read yes
```

### Display SmartIO cache information for directory /vx/tpcc_data1

```
SmartIO> file list /vx/tpcc_data1
/vx/tpcc_data1:
READ CACHE WRITEBACK MODE PINNED NAME
16.68 MB 0 KB read no /vx/tpcc_data1/cntrlSLOB.ctl
18.26 MB 0 KB read no /vx/tpcc_data1/o1_system.dbf
14.8 MB 0 KB read no /vx/tpcc_data1/o1_sysaux.dbf
2.009 GB 0 KB read no /vx/tpcc_data1/o1_mf_iops.dbf
2.04 GB 0 KB read no /vx/tpcc_data1/SLOB/datafile
0 KB 0 KB read yes /vx/tpcc_data1/control1.ctl
16.68 MB 0 KB read yes /vx/tpcc_data1/system.dbf
2.07 GB 0 KB read no /vx/tpcc_data1
```

### See Also

cache(1), fs(1), file(1)
15.2 cache

15.2.1 SYNOPSIS

```bash
cache create node_name disk size fstype cachename
cache delete node_name cache_name
cache grow cache_size node_name cache_name
cache list
cache offline node_name cache_name
cache online node_name cache_name
cache shrink cache_size node_name cache_name
cache stat node_name
cache wb_size node_name cache_name cache_size
```

15.2.2 DESCRIPTION

The SmartIO cache commands are used to create and manage the SmartIO cache. The cache commands let you create, delete, or resize the SmartIO cache. You can bring the SmartIO cache online or offline. You can view the statistics of the SmartIO cache usage and list the cache properties. You must specify the `node_name` as one of the arguments, because the SmartIO cache is local to a node. Veritas Access supports multiple cache creations.

15.2.3 OPTIONS

- **cache create node_name disk size fstype cachename**  
  Create the SmartIO cache on the `cache_name` using the specified SSD disk.

- **cache delete node_name cache_name**  
  Delete the specified SmartIO cache on the specified node.

- **cache grow cache_size node_name cache_name**  
  Grow the specified SmartIO cache on the specified node. The `cache_size` is specified in GB or TB.

- **cache list**  
  List the SmartIO cache properties on the specified node.

- **cache offline node_name cache_name**  
  Bring the SmartIO cache offline on the specified node.

- **cache online node_name cache_name**  
  Bring the SmartIO cache online on the specified node.

- **cache shrink cache_size node_name cache_name**  
  Shrink the SmartIO cache on the specified node. The `cache_size` is specified in GB or TB.

- **cache stat node_name**  
  Display the SmartIO cache statistics on the specified node.

- **cache wb_size node_name cache_name cache_size**  
  Set the SmartIO cache writeback size.
15.2.4 EXAMPLES

Create a SmartIO cache.

```
 test1.SmartIO> cache create sdb,sdc 2G reserve cache6
 SmartIO cache area created
```

List the SmartIO cache properties.

```
 test1.SmartIO> cache list

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>SIZE</th>
<th>ASSOC-TYPE</th>
<th>STATE</th>
<th>FSTYPE</th>
<th>DEVICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache4</td>
<td>VxFS</td>
<td>2.00g</td>
<td>AUTO</td>
<td>OFFLINE</td>
<td>default</td>
<td>sdb</td>
</tr>
<tr>
<td>cache6</td>
<td>VxFS</td>
<td>2.00g</td>
<td>AUTO</td>
<td>ONLINE</td>
<td>reserve</td>
<td>sdb,sdc</td>
</tr>
</tbody>
</table>
```

Bring the SmartIO cache online.

```
 test1.SmartIO> cache online test1_01 cache6
 SmartIO cache is online
```

Grow the SmartIO cache.

```
 test1.SmartIO> cache grow 16g test1_01 cache2
 Smartio cache grow completed
```

Change the fstype of SmartIO cache.

```
 test1.SmartIO> cache settype clusA_01 cache5 reserve
 ACCESS smartio SUCCESS V-288-999 SmartIO cache fstype change
```

Display SmartIO cache statistics.

```
 test1.SmartIO> cache stat

 TYPE: VxFS
 NAME: cachel
 Cache Size: 15.97 GB
 Cache Utilization: 118.0 MB (0.72 %)
 File Systems Using Cache: 7
 Writeback Cache Use Limit: Unlimited
 Writeback Flush Timelag: 10 s

<table>
<thead>
<tr>
<th>Read Cache</th>
<th>Writeback</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hit Ratio</td>
<td>Hit Ratio</td>
</tr>
<tr>
<td>Data Read</td>
<td>Data Written</td>
</tr>
<tr>
<td>8.97 %</td>
<td>0.00 %</td>
</tr>
<tr>
<td>52 KB</td>
<td>0 KB</td>
</tr>
<tr>
<td>/shared</td>
<td></td>
</tr>
<tr>
<td>8.97 %</td>
<td>0.00 %</td>
</tr>
<tr>
<td>52 KB</td>
<td>0 KB</td>
</tr>
</tbody>
</table>

Set the SmartIO cache writeback size.

```
 test1.SmartIO> cache wb_size sun_01 cache6 8g
 ACCESS smartio SUCCESS V-288-999 SmartIO WB cache set to 8g
```
15.2.5 SEE ALSO

cache(1), fs(1), file(1)
15.3 device

15.3.1 SYNOPSIS

device list node_name

15.3.2 DESCRIPTION

The SmartIO device command is used to list all available SSD devices on node_name.

The device command lets you list all available SSD devices on node_name. You must specify the node_name as one of the arguments, because the SmartIO device is local to a node.

15.3.3 OPTIONS

    device list node_name List the SSD devices available on node_name.

15.3.4 EXAMPLES

List SSD Devices:

```plaintext
SNODE.SmartIO> device list test1_01
NODE-NAME = test1_01
=================
DEVICE STATUS
==== =====
intel_ssd0_0 online
intel_ssd1_0 online
intel_ssd2_0 online
```

15.3.5 SEE ALSO

cache(1), fs(1), file(1)
15.4 file

15.4.1 SYNOPSIS

file cachemode {nocache|read|writeback} file_name
file list file_name
file load file_name
file pin file_name
file restore_access file_name
file unpin file_name

15.4.2 DESCRIPTION

The SmartIO file commands are used to set cache policies, list current cache policies at file or directory. The argument file_name refers to a single file or directory name. You can load, pin and unpin specified files into the SmartIO cache. The writeback cache policy is supported on two node Veritas Access clusters only.

15.4.3 OPTIONS

file cachemode {nocache|read|writeback} file_name  Set caching mode for the named file or directory. The supported caching mode are read, nocache or writeback. For directories, caching mode is set recursively.

file load file_name  Load the named file or directory into the SmartIO cache. The file is loaded asynchronously in background.

file pin file_name  Pin the named file or directory into SmartIO cache. The pinned file blocks in the cache generally will not be aged out of the cache.

file list file_name  List the SmartIO cache properties for the specified file_name.

file restore_access file_name  Enables access to files that are missing writeback data. If the writeback cache data could not be flushed to the disk for some files due to an error, SmartIO prevents access to the files. This command only restores access to the files, but it does not restore the missing data.

file unpin file_name  Unpin the named file or directory into smartIO cache.

15.4.4 EXAMPLES

Load the system.dbf file into the SmartIO cache.

SmartIO> file load /vx/tpcc_data/system.dbf
SUCCESS : SmartIO cache load for /vx/tpcc_data1/system.dbf on host ISAGA_01

Pin the system.dbf file into SmartIO cache.

SmartIO> file pin /vx/tpcc_data/system.dbf
SUCCESS : SmartIO cache pin for /vx/tpcc_data1/system.dbf

Display SmartIO information for file system.dbf.
Display SmartIO cache information for directory /vx/tpcc_data1.

15.4.5 SEE ALSO

cache(1), fs(1), file(1)
15.5 fs

15.5.1 SYNOPSIS

fs cachemode {nocache | read | writeback} fs_name
fs disable fs_name
fs enable fs_name
fs flush fs_name
fs list fs_name
fs purge fs_name
fs stat fs_name

15.5.2 DESCRIPTION

The SmartIO file system level commands are used to enable, disable, flush, or purge the SmartIO cache for the file system specified by fs_name. The cachemode command lets you set the caching policy for the entire file system. The possible cachemodes are read, nocache, and writeback.

15.5.3 OPTIONS

fs cachemode {nocache | read | writeback} fs_name Set read, nocache or writeback SmartIO cache policy for fs_name file system.
fs disable fs_name Disable SmartIO cache for the fs_name file system. This action stops SmartIO cache for the file system specified.
fs enable fs_name Enable SmartIO cache for the fs_name file system. This action starts caching for the specified file system.
fs flush fs_name Flush the writeback data for the fs_name file system. For this command to work, the file system must be configured with writeback cache.
fs list fs_name Display the SmartIO cache properties and usage for the fs_name file system.
fs purge fs_name Purge or remove the cached contents for the fs_name file system in SmartIO cache.
fs stat fs_name Display detailed SmartIO cache statistics for the fs_name file system specified.

15.5.4 EXAMPLES

Set the nocache SmartIO policy for file system where TPCC database archivelog files are stored.

SmartIO> fs cachemode nocache tpcc_arch1
Cluster-configuration updated with changed Mount Options for node test_01
Mount Point /vx/tpcc_arch1 remounted successfully on test_01
Cluster-configuration updated with changed Mount Options for node test_02
Mount Point /vx/tpcc_arch1 remounted successfully on test_02
Enable the SmartIO cache for file system where TPCC data files are stored.

SmartIO> fs enable tpcc_data1

List the SmartIO cache for file system tpcc_data1.

SmartIO> fs list tpcc_data1
/vx/tpcc_data1:
READ CACHE WRITEBACK MODE PINNED NAME
 648 KB   0 KB   read no       /vx/tpcc_data1/cntrlSLOB.ctl
  0 KB   0 KB   read no       /vx/tpcc_data1/SLOB
 648 KB   0 KB   read no       /vx/tpcc_data1

List SmartIO cache for file system tpcc_data1.

SmartIO> fs stat tpcc_data1
    Cache Size: 15.97 GB
Cache Utilization: 652 KB ( 0.00 %)
Read Cache
Hit Ratio Data Read Data Written
/vx/tpcc_data1:
 96.40 %  12.55 MB  1.656 MB
/vx/tpcc_data1:

15.5.5 SEE ALSO

cache(1), fs(1), file(1)
16.1 Storage

16.1.1 SYNOPSIS

pool create pool_name disk1 [ , disk2,...] [isolated={yes|no}]
npool adddisk pool_name disk1 [ , disk2,...]
pool destroy pool_name
pool free [pool_name]

pool list
pool markdiskspare pool_name disk1 [ , disk2,...]
pool removediskspare pool_name disk1 [ , disk2,...]
disk configure local <nodename> <vendor_id> <product_id> [serial_num]

pool mvdisk src_pool dest_pool disk1 [ , disk2,...]
pool rename old_name new_name

pool rmdisk disk1 [ , disk2,...]
disk list [ stats | detail | paths ]
disk grow disk_name
disk format disk_name [ , disk2,...] [force]
hba [host_name]
fencing destroy

fencing on disk [disk1, disk2, disk3]
fencing on majority
fencing off
fencing replace src_disk fildest_disk
fencing status
fs create simple 
\[fs\_name\ size pool1 \[,\ disk1,\ldots\] \[blksz=\text{<bytes>}\] \[pdir\_enable={yes|no}\] \[encrypt={on|off}\] \[worm={yes|no}\] \]

fs create mirrored 
\[fs\_name\ size nmirrors pool1 \[,\ disk1,\ldots\] \[protection=disk|pool\] \[blksize=\text{<bytes>}\] \[pdir\_enable={yes|no}\] \[encrypt={on|off}\] \[worm={yes|no}\] \]

fs create striped 
\[fs\_name\ size ncolumns pool1 \[,\ disk1,\ldots\] \[blksize=\text{<bytes>}\] \[pdir\_enable={yes|no}\] \[encrypt={on|off}\] \[worm={yes|no}\] \]

fs create mirrored-stripe 
\[fs\_name\ size nmirrors ncolumns pool1 \[,\ disk1,\ldots\] \[protection=disk|pool\] \[blksize=\text{<bytes>}\] \[pdir\_enable={yes|no}\] \[encrypt={on|off}\] \[worm={yes|no}\] \]

fs create largefs simple 
\[fs\_name\ size pool1 \[blksz=\text{<bytes>}\] \]

fs create largefs mirrored 
\[fs\_name\ size nmirrors pool1 \[blksz=\text{<bytes>}\] \]

fs create largefs striped 
\[fs\_name\ size ncolumns pool1 \[stripeunit=\text{kilobytes}\] \[blksize=\text{<bytes>}\] \]

fs create largefs mirrored-stripe 
\[fs\_name\ size nmirrors ncolumns pool1 \[stripeunit=\text{kilobytes}\] \[blksize=\text{<bytes>}\] \]

fs create pretuned 
\[fs\_name\ size pool1 \ workloads\{virtualmachine|mediaserver\} \[layout=\{striped|striped-mirror|mirrored-stripe\}\] \[ncolumns\] \[encrypt={on|off}\] \]

fs defrag now \[fs\_name\ time\] 

fs destroy \[fs\_name\] 

fs list \[fs\_name\] 

fs online \[fs\_name\] 

fs offline \[fs\_name\] 

fs growto \[primary\|secondary\] \[fs\_name\ new_length pool1 \[,\ disk1,\ldots\]\] \[protection=disk|pool\] 

fs growby \[primary\|secondary\] \[fs\_name\ length\_change pool1 \[,\ disk1,\ldots\]\] \[protection=disk|pool\] 

fs shrinkto \[primary\|secondary\] \[fs\_name\ new_length\] 

fs shrinkby \[primary\|secondary\] \[fs\_name\ length\_change\] 

fs addmirror \[fs\_name\ pool1 \[,\ disk1,\ldots\]\] \[protection=disk|pool\] 

fs rmmirror \[fs\_name\ pool\_or\_disk\_name\] 

fs addcolumn \[fs\_name\ ncolumns pool\_or\_disk\_name\] 

fs rmcolumn \[fs\_name\] 

fs checkmirror 

fs resync \[fs\_name\] 

fs checkresync 

fs setfastresync \[fs\_name\ pool\_or\_disk\_name\] 

fs unsetfastresync \[fs\_name\] 

fs fsck \[fs\_name\] 

cloud addservice \[service\_name\ \[service\_provider=\text{<service\_provider>}\] \]
cloud listservice [service_name]
cloud removeservice service_name
tier add simple fs_name size pool1 [ disk1, ...]
tier add mirrored fs_name size nmirrors pool1 [ disk1, ...] [protection=disk|pool]
tier add striped fs_name size ncolumns pool1 [ disk1, ...]
tier add mirrored-stripe fs_name size nmirrors ncolumns pool1 [ disk1, ...] [protection=disk|pool]
tier add striped-mirror fs_name size nmirrors ncolumns pool1 [ disk1, ...] [protection=disk|pool]
tier addcolumn fs_name ncolumns pool1 [ disk1, ...]
tier add cloud fs_name tier_name service_name region S3|Glacier
tier remcolumn fs_name
tier remove fs_name [tier_name]
tier addmirror fs_name pool1 [ disk1, ...] [protection=disk|pool]
tier rmmirror fs_name [pool_or_disk_name]
tier listfiles fs_name (primary|secondary)
tier mapfile fs_name file_path
tier policy list
tier policy prune list
tier policy prune modify fs_name delete_after
tier policy modify fs_name (primary|secondary) days minacctemp period
tier relocate fs_name dirPath
tier policy remove fs_name
tier policy prune remove fs_name
tier policy run fs_name
tier schedule list
tier schedule modify fs_name minute hour day_of_the_month month day_of_the_week node_name
tier schedule remove fs_name
tier query fs_name
tier setfastresync fs_name pool1 [ disk1, ...]
tier unsetfastresync fs_name
tier stats monitor fs_name tier_name [interval]
tier stats (show|reset|usage) fs_name tier_name
scanbus
snapshot create snapshot_name fs_name [removable=yes|removable=no]
snapshot restore snapshot_name fs_name
snapshot destroy snapshot_name fs_name
snapshot list [fs_name]
snapshot online snapshot_name fs_name
snapshot offline snapshot_name fs_name
snapshot quota on fs_name [capacity_limit]
snapshot quota off [fs_name]
snapshot quota list
snapshot schedule create schedule_name fs_name max_snapshot_limit minute hour day_of_the_month month day_of_the_week
snapshot schedule modify schedule_name fs_name max_snapshot_limit minute hour day_of_the_month month day_of_the_week
snapshot schedule destroyall schedule_name fs_name
snapshot schedule preserve schedule_name fs_name snapshot_name
snapshot schedule show [fs_name] [schedule_name]
snapshot schedule delete fs_name [schedule_name]
iscsi status
iscsi start
iscsi stop
iscsi device add device
iscsi device del device
iscsi device list
iscsi discovery add discovery-address
iscsi discovery del discovery-address
iscsi discovery rediscover discovery-address
iscsi discovery rediscover_new discovery-address
iscsi discovery list
iscsi target add target-name portal-address
iscsi target del target-name { discovery-address | portal-address }
iscsi target login target-name { discovery-address | portal-address }
iscsi target logout target-name { discovery-address | portal-address }
iscsi target rescan target-name
iscsi target attr showdefault
iscsi target attr showall
iscsi target attr show target-name
iscsi target attr setdefault attribute value
iscsi target attr setall attribute value
iscsi target attr set target-name attribute value
iscsi target list
iscsi target listdetail target-name
iscsi initiatorname set initiatorname-prefix
iscsi initiatorname list
quota fs enable fs_name [userquota | groupquota]
quota fs disable fs_name [userquota | groupquota]
quota fs status fs_name [userquota | groupquota]
quota fs set userquota | groupquota user_or_group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs setbygroup group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs show fs_name [userquota | groupquota] [user_or_group_names] [domain_name]
quota fs setdefault userquota | groupquota hardlimit | softlimit numinodes | numspace [value] [fs_name]
quota fs showdefault fs_name [userquota | groupquota]
quota cifshomedir enable [userquota | groupquota]
quota cifshomedir disable [userquota | groupquota]
quota cifshomedir status [userquota | groupquota]
quota cifshomedir set userquota | groupquota user_or_group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value]
quota cifshomedir setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value]
quota cifshomedir show [userquota | groupquota] [user_or_group_names] [domain_name]
quota cifshomedir showdetail [userquota | groupquota] [user_or_group_names] [domain_name]
quota cifshomedir setdefault userquota | groupquota hardlimit | softlimit numinodes | numspace [value]
quota cifshomedir showdefault fs_name [userquota | groupquota]
dedup enable fs_name [blksize]
dedup disable fs_name
dedup list fs_name
dedup start fs_name [node_name]
dedup stop fs_name
dedup status fs_name
dedup set cpu cpuvalue fs_name
dedup set memory memvalue
dedup set priority priorityval fs_name
dedup schedule set fs_name hours day [freq]
dedup schedule modify fs_name hours day [freq]
dedup schedule delete fs_name

dedup dryrun fs_name [threshold]

dedup remove fs_name

compress file fs_name {file|dir} <res_level> [alg_strength] [file_pattern]

compress list fs_name {file|dir}

uncompress file fs_name {file|dir} <res_level>

compress modage create fs_name age_rule

compress modage remove fs_name

compress pattern create fs_name pattern_rule

compress pattern remove fs_name

compress schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]

compress schedule remove sched_name

compress schedule show [sched_name]

compress schedule start fs_name sched_name res_level [alg_strength]

compress schedule stop fs_name

compress schedule list fs_name

fs defrag schedule create sched_name duration minute [hour] [day] [month] [day_of_the_week] [node]

fs defrag schedule remove sched_name

fs defrag schedule show [sched_name]

fs defrag schedule start fs_name sched_name

fs defrag schedule stop fs_name

fs defrag schedule list fs_name

fs policy add operation=move policy_name fs_name from_tier to_tier retrieval_option=Expedited|Standard|Bulk pattern [atime condition] [mtime condition]

fs policy add operation=delete policy_name fs_name from_tier pattern [atime condition] [mtime condition]

fs policy modify policy_name pattern [atime condition] [mtime condition]

fs policy delete policy_name fs_name

fs policy rename old_policy_name new_policy_name

fs policy list [fs_name]

fs policy run policy_name

fs policy dryrun policy_name

fs policy status policy_name

fs policy abort policy_name

fs policy pause policy_name

fs policy resume policy_name

fs policy schedule create fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
fs policy schedule modify fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
fs policy schedule remove fs_name
fs policy schedule list fs_name
fs retention set path rtime
fs retention show path
fs retention clear path
fs worm set fs_name
fs worm clear fs_name

16.1.2 DESCRIPTION

The storage commands create logical pools and file systems.

File systems consist of metadata and file data. Metadata consists of information like last modification time, creation time, permissions, and so on. The total amount of space taken by the metadata depends upon the number of files. A file system that contains many smaller files requires more space to store the metadata, and a file system with fewer large files requires less space to store the metadata.

When a file system is created, some space is set aside initially for the metadata. This space is generally proportional to the size of the file system. This is the reason for the non-zero usage percentage in the output of fs list just after the creation of the file system. The space that was set aside for the metadata would grow or shrink as and when required. A file system on a 1 GB volume would take around 40 MB (about 4%) initially for storing the metadata, whereas a file system of size 10 MB would take around 7.3 MB (73%) initially for storing the metadata.

16.1.3 OPTIONS

device

Device on which the operation takes place.

target-name

Name of the iSCSI target at which SCSI LUNs are available. target-name should conform to the naming rules defined in RFC3721.

encrypt={yes|no}

Specify whether to create the file system on encrypted volume. If set to on, file system is created on encrypted volume. The default value is encrypt=off.

pdir_enable={yes|no}

Enable or disable partition directory for the file system. The default value is pdir_enable=no, which means partition directory is disabled for the file system.

worm={yes|no}

Specify whether to create a worm-enabled file system. If set to yes, file system is created with WORM support enabled. The default value is worm=no.

workload={virtualmachine|mediaserver}

Type of workload using this file system. The workload type cannot be changed after the file system is created. If the workload type is virtualmachine, then all the files in the file system have a minimum extent size of 1 MB. This reduces file system fragmentation and improves virtual machine I/O performance.
layout={striped|striped-mirror|mirrored-stripe}

Layout of the underlying volume on which the file system is created. The default value is layout=striped.

discovery-address

Discovery address is the target address at which the initiator can request a list of targets using SendTarget’s text request as specified in the iSCSI protocol of RFC3720. If no port is specified with the discovery address, the default port 3260 is used. IPv4 and IPv6 addresses are supported. Examples:

<table>
<thead>
<tr>
<th>Address 1</th>
<th>Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.4</td>
<td>192.168.0.4:3260</td>
</tr>
<tr>
<td>2001:c90::211:9ff:feb8:a9e9</td>
<td>[2001:c90::211:9ff:feb8:a9e9]:3260</td>
</tr>
</tbody>
</table>

initiatorname-prefix

initiatorname-prefix is a name that conforms to the naming rules for initiator and target names as specified in RFC3721. Initiator names for nodes in the cluster are generated by appending the node number to this prefix.

portal-address

Portal address is the location at which the target is accessible. IPv4 and IPv6 addresses are supported. Examples:

<table>
<thead>
<tr>
<th>Address 1</th>
<th>Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.4</td>
<td>192.168.0.4,1</td>
</tr>
<tr>
<td>192.168.0.4:3260</td>
<td>192.168.0.4:3260,1</td>
</tr>
<tr>
<td>2001:c90::211:9ff:feb8:a9e9</td>
<td>2001:c90::211:9ff:feb8:a9e9,1</td>
</tr>
<tr>
<td>[2001:c90::211:9ff:feb8:a9e9]:3260</td>
<td>[2001:c90::211:9ff:feb8:a9e9]:3260,10</td>
</tr>
</tbody>
</table>

pool create pool_name disk1 [, disk2,...] [isolated={yes|no}]

Create a logical pool from a given set of disks. If isolated=yes, then a new disk group is created. The default value for isolated is isolated=no.

pool adddisk pool_name disk1 [, disk2,...]

Add a set of disks to a logical pool.

pool destroy pool_name

Destroy a pool.

pool free [pool_name]

List free space in each of the pools.

pool list

List all the pools.

pool mvdisk src_pool dest_pool disk1 [, disk2,...]

Move disks from one pool to another.

pool rename old_name new_name

Rename a pool.

pool rmdisk disk1 [, disk2,...]
Remove disks from a pool.

```plaintext
pool markdiskspare pool_name disk1 [, disk2,...]
```

Mark a disk as a spare disk and add it to a pool which is later used for hot-relocation. In case of failure of a disk or a plex, the affected subdisks are relocated to disks designated as spare disks.

```plaintext
pool removediskspare pool_name disk1 [, disk2,...]
```

Remove the spare disk flag set on a disk by markdiskspare command.

disk list stats

Display the aggregated information of all the disks.

disk list detail

Display properties of all the disks.

disk list paths

Display the list of multiple paths of all the disks from all the nodes in the cluster.

disk configure local <nodename> <vendor_id> <product_id> [serial_num]

Add local disks having the specified vendor ID and product ID in the JBOD category.

disk grow disk_name

Increase the size of the specified disk. Before performing this operation make sure that you increase the storage capacity of the disk on the storage array. **Caution:** When increasing the storage capacity of a disk, make sure that the storage array does not reformat it. This will destroy the data. For help, contact your Storage Administrator.

disk format disk1 [, disk2,...] [force]

If the disk does not belong to any disk group, the format option erases the first 100 M space on the disk, and the disk is formatted using the vxdisksetup command. Use the force option to force formatting of disks with invalid configurations.

hba [host_name]

Display World Wide Name (WWN) information of all or a specified node of the cluster.

fencing destroy

Destroy coordinator pool. This command has no effect for majority-based fencing.

fencing on disk [disk1, disk2, disk3]

Enable I/O fencing on the three disks (only three disks required).

fencing on majority

Enable majority-based I/O fencing.

fencing off

Disable I/O fencing on all the nodes.

fencing replace src_disk dest_disk

Replace an existing coordinator disk with another disk. If the disk being replaced is in a failed state, then it is mandatory to delete the disk from the array. This is required because if the failed disk comes up and works properly, it can lead to an even number of I/O fencing disks, and this affects the functionality. This command has no effect for majority-based I/O fencing.

fencing status

16.1. storage
Check I/O fencing status.

```
fs create simple fs_name size pool1 [, disk1,...] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]
```

Create a simple file system with a specified size on one of the specified pools/disks and make it online.

```
fs create mirrored fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]
```

Create a mirrored file system with a specified number of mirrors and make it online.

```
fs create striped fs_name size ncolumns pool1 [, disk1,...] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]
```

Create a striped file system with a specified number of stripes and make it online.

```
fs create mirrored-stripe fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]
```

Create a mirrored-striped file system with a specified number of mirrors and stripes and make it online.

```
fs create striped-mirror fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]
```

Create a striped-mirrored file system with a specified number of mirrors and stripes and make it online.

```
fs create largefs simple fs_name size pool1 [blksize=<bytes>]
```

Create a largefs file system with the specified size on pools/disks specified and bring it online.

```
fs create largefs mirrored fs_name size nmirrors pool1 [blksize=<bytes>]
```

Create a mirrored largefs file system with the specified number of mirrors and make it online.

```
fs create largefs striped fs_name size ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a striped largefs file system with the specified number of stripes and make it online.

```
fs create largefs mirrored-stripe fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a mirrored-striped largefs file system with a specified number of mirrors and stripes and make it online.

```
fs create largefs striped-mirror fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a striped-mirrored largefs file system with a specified number of mirrors and stripes and make it online.

```
fs create pretuned fs_name size pool1 workload={virtualmachine|mediaserver} [layout={striped|striped-mirror|mirrored-stripe}] [ncolumns] [encrypt={on|off}]
```

Create a file system with the specified size using the disks from the specified pool. The volume is created with the specified layout. Stripe the volume across the specified number of columns with 512 K as the stripe size. Tune the file system for the specified workload.

```
fs defrag now fs_name time
```

Defragment a file system now. The `time` value should be larger than 1 minute or infinite.

```
fs destroy fs_name
```

Destroy a file system.

```
fs list [fs_name]
```
List all the file systems.

```
fs online fs_name
```

Make the file system online.

```
fs offline fs_name
```

Make the file system offline.

```
fs growto primary|secondary fs_name new_length [pool1 [, disk1,...]] [protection=disk|pool]
```

Grow the file system’s primary or secondary tier to a specified size. Or grow the largefs file system’s primary disk tier to a specified size.

```
fs growby primary|secondary fs_name length_change [pool1 [, disk1,...]] [protection=disk|pool]
```

Grow the file system’s primary or secondary tier by a specified size. Or grow the largefs file system’s primary disk tier by a specified size.

```
fs shrinkto primary|secondary fs_name new_length
```

Shrink the file system’s primary or secondary tier to a specified size. Or shrink the largefs file system’s primary disk tier to a specified size.

```
fs shrinkby primary|secondary fs_name length_change
```

Shrink the file system’s primary or secondary tier by a specified size. Or shrink the largefs file system’s primary disk tier by a specified size.

```
fs addmirror fs_name pool1 [, disk1,...] [protection=disk|pool]
```

Add a mirror to the file system.

```
fs rmmirror fs_name [pool_or_disk_name]
```

Remove a mirror from the file system that is spanning on the specified pools and disks.

```
fs addcolumn fs_name ncolumns pool_or_disk_name
```

Add the specified number of columns to the file system. In case of a striped file system, the number of disks specified should be equal to ncolumns. In case of mirrored-stripe and striped-mirror, the disks specified should be equal to (ncolumns * number_of_mirrors_in_fs)

```
fs rmcolumn fs_name
```

Remove a column from the file system.

```
fs checkmirror
```

Show file systems that have stale mirrors.

```
fs resync [fs_name]
```

Resynchronize all stale mirrors for all file systems or for a certain file system.

```
fs checkresync
```

Show resynchronization progress running in the background.

```
fs setfastresync fs_name [pool_or_disk_name]
```

Enable fast resync for the specified file system.

```
fs unsetfastresync fs_name
```

Disable fast resync for the specified file system.

```
fs fsck fs_name
```

16.1. storage
Check and repair the specified file system.

```
cloud addservice service_name [service_provider=<service_provider>]
```

Add a public cloud subscription to Veritas Access as a cloud service with a name. The added subscription is accessed using `service_name` thereafter. You are prompted to provide the subscription credentials. Credentials are verified and the cloud service is added.

```
cloud listservice [service_name]
```

List added cloud services. If `service_name` is provided, then only that cloud service is listed. Otherwise all configured services are listed.

```
cloud removeservice service_name
```

Remove the cloud service `service_name`.

**Warning:** Service removal fails if there are active cloud tiers associated with this service at time of removal.

```
tier add simple fs_name size pool1 [, disk1,...]
```

Add a simple tier to the specified file system on one of the specified pools and disks.

```
tier add mirrored fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool]
```

Add a mirrored tier to the specified file system.

```
tier add striped fs_name size ncolumns pool1 [, disk1,...]
```

Add a striped tier to the specified file system.

```
tier add mirrored-stripe fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool]
```

Add a mirrored-stripe tier to the specified file system.

```
tier add striped-mirror fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool]
```

Add a striped-mirror tier to the specified file system.

```
tier addcolumn fs_name ncolumns pool1 [, disk1,...]
```

Add a column to the tier of the file system.

```
tier add cloud fs_name tier_name service_name region S3|Glacier
```

Add a cloud tier to the specified scale-out file system using service name and region. You can specify if you want to add an S3-compatible or Glacier cloud storage tier by specifying the appropriate option. S3-compatible is any third-party implementation of the Amazon S3 APIs (Supporting Signature version 4 signing).

The supported regions of the Amazon S3 service are the following:

- California (us-west-1)
- Central (ca-central-1)
- Frankfurt (eu-central-1)
- Ireland (eu-west-1)
- London(eu-west-2)
- Mumbai (ap-south-1)
- Ohio (us-east-2)
- Oregon (us-west-2)
Veritas Access Command Reference Guide Documentation, Release 7.3

- Seoul (ap-northeast-2)
- Singapore (ap-southeast-1)
- Sydney (ap-southeast-2)
- SaoPaulo (sa-east-1)
- Tokyo (ap-northeast-1)
- Virginia (us-east-1)

Region is irrelevant to an S3-compatible cloud storage service. If you select an S3-compatible service, select “none” as the region. Any other region specified with an S3-compatible is ignored.

**Warning:** When a cloud storage service is used as a cloud tier for a scale-out file system, Veritas Access exclusively owns all the buckets and the objects created by Veritas Access. Any attempt to tamper with these buckets or objects outside of Veritas Access corrupts the files represented by those modified objects.

tier rmcolumn fs_name

Remove a column from the tier of the file system.

tier remove fs_name [tier_name]

Remove a tier from the file system. All files on the secondary tier get relocated to the primary tier. Ensure that you remove the policy by running tier policy remove <fs_name> before running the tier remove command.

tier addmirror fs_name pool1 [, disk1,...] [protection=disk|pool]

Add a mirror to the tier of the file system.

tier rmmirror fs_name [pool_or_disk_name]

Remove a mirror from the tier of the file system that is spanning on the specified pools and disks.

tier listfiles fs_name (primary|secondary)

Show all the files that are on the specified tier.

tier mapfile fs_name file_path

Show the tier location of the specified file. The path of the file is relative to the file system. For example, tier mapfile fs1 /a.txt would show the location of a.txt, which is in the root directory of the file system fs1.

tier policy list

Show policy for each tiered file system.

tier policy prune list

Show prune policy for each tiered file system.

tier policy prune modify fs_name delete_after

Change the prune policy of the tiered file system.

tier policy modify fs_name (primary|secondary) days minacctemp period

Change the policy of the tiered file system.

tier relocate fs_name dirPath

Relocate the directory or the file from the secondary tier to the primary tier. This does not relocate NDS (Named Data Stream also includes extended attributes) to the primary tier.

tier policy remove fs_name
Remove the policy of the tiered file system.

\texttt{tier policy prune remove fs\_name}

Remove the prune policy of the tiered file system.

\texttt{tier policy run fs\_name}

Run the policy of the tiered file system.

\texttt{tier schedule list}

Show schedules of all the tiered file systems.

\texttt{tier schedule modify fs\_name minute hour day\_of\_the\_month month day\_of\_the\_week node\_name}

Modify the schedule of the tiered file system.

\texttt{tier schedule remove fs\_name}

Remove the schedule of the tiered file system.

\texttt{tier query fs\_name}

Show the list of files that will be moved by running the policy.

\texttt{tier setfastresync fs\_name pool1 [disk1,...]}

Set fastresync for the tier of the file system.

\texttt{tier unsetfastresync fs\_name}

Unset fastresync for the tier of the file system.

\texttt{tier stats \{show\|reset\|usage\} fs\_name tier\_name}

Show the access statistics, reset the access statistics to zero, or show the total usage of the specified cloud tier in the largefs file system.

\texttt{tier stats monitor fs\_name tier\_name \[interval\]}

Monitor the access statistics of the specified cloud tier in the largefs file system. The default interval is five seconds.

\texttt{scanbus}

Scan all the SCSI devices connected to all or a specified node of the cluster.

\texttt{snapshot create snapshot\_name fs\_name \[removable=yes\|removable=no\]}

Create a snapshot for a specified file system. If the removable attribute is \texttt{yes} and if it is offline, then it is removed automatically, if the file system runs out of space.

\texttt{snapshot restore snapshot\_name fs\_name}

Restore a file system by a given snapshot.

\texttt{snapshot destroy snapshot\_name fs\_name}

Destroy the snapshot of a file system.

\texttt{snapshot list \[fs\_name\]}

Displays all the snapshots of the specified file system. If no file system is specified, snapshots of all the file systems are displayed.

\texttt{snapshot online snapshot\_name fs\_name}

Make the snapshot online.
snapshot offline snapshot_name fs_name

Make the snapshot offline.

snapshot quota on fs_name [capacity_limit]

Disallow creation of snapshots on the given file system when the space used by all the snapshots of that file system exceeds a given capacity limit. The space used by the snapshots is not restricted.

snapshot quota off [fs_name]

Disable quota capacity limit for a specified system.

snapshot quota list

Display snapshot quota information of all the file systems.

snapshot schedule create schedule_name fs_name max_snapshot_limit minute hour day_of_the_month month year day_of_the_week

Create schedule for automated snapshot creation of a particular file system.

snapshot schedule modify schedule_name fs_name max_snapshot_limit minute hour day_of_the_month month year day_of_the_week

Modify schedule for automated snapshot creation of a particular file system.

snapshot schedule destroyall schedule_name fs_name

Destroy all automated snapshots corresponding to a given schedule name and file system name (excluding the preserved and online snapshots).

snapshot schedule preserve schedule_name fs_name snapshot_name

Preserve a limited number of snapshots corresponding to an existing schedule and a specific file system name so that they are not removed as part of the snapshot schedule autoremove command.

snapshot schedule show [fs_name] [schedule_name]

Show all schedules that have been set for automated snapshot creation.

snapshot schedule delete fs_name [schedule_name]

Deletes the schedule set for automated snapshot creation for a particular file system or for a particular schedule.

iscsi status

Shows the status of the iSCSI initiator service.

iscsi start

Starts the iSCSI initiator service.

iscsi stop

Stops the iSCSI initiator service.

iscsi device add device

Add a device for use with the iSCSI initiator. iSCSI initiator connections use this device to connect to the target. If there are any existing targets, then the iSCSI initiator initiates a connection to all the targets using device.

iscsi device del device
Delete a device from the iSCSI initiator configuration. Any existing connections from device to targets is terminated. If device is the last device in the iSCSI initiator configuration and there are existing targets, then the device cannot be deleted from the configuration.

```bash
iscsi device list
List the devices used by the iSCSI initiator.
```

```bash
iscsi discovery add discovery-address
Add a discovery address to the iSCSI initiator configuration. If no TCP port is specified with the discovery-address, then the default port 3260 is used. Any targets discovered at discovery-address are automatically logged on to.
```

```bash
iscsi discovery del discovery-address
Delete a discovery address from an iSCSI initiator configuration. Any targets discovered using discovery-address are also deleted from the configuration.
```

```bash
iscsi discovery rediscover discovery-address
Perform a discovery of changes in targets or LUNs at discovery-address. Any LUNs or targets that have been removed at discovery-address are automatically removed from the configuration. New LUNs or targets discovered at discovery-address are automatically added and logged on to.
```

```bash
iscsi discovery rediscover_new discovery-address
Perform a discovery of changes in targets or LUNs at discovery-address. New LUNs or targets discovered at discovery-address are automatically added and logged on to. Does not discover any targets that have been deleted at fldiscovery-address.
```

```bash
iscsi discovery list
List the discovery addresses present in the iSCSI initiator configuration.
```

```bash
iscsi target add target-name portal-address
Add a static target-portal combination to the iSCSI initiator configuration. The portal-address cannot be the same as any discovery-address present in the iSCSI initiator configuration. Connections to portal-address are made for target-name, but no discovery is done for any other targets available at portal-address. If no portal tag is specified with portal-address, the default portal tag of 1 is used.
```

```bash
iscsi target del target-name { discovery-address | portal-address }
Delete a target target-name from the iSCSI initiator configuration. Any existing connections to target-name are terminated. discovery-address or portal-address is the address through which the target became visible to the initiator. A target that was discovered at a discovery-address once deleted from the iSCSI initiator configuration would again be visible to the iSCSI initiator if re-discovery is done either through iscsi discovery rediscover or scanbus commands.
```

```bash
iscsi target login target-name { discovery-address | portal-address }
Logon to a target target-name from the iSCSI initiator. Connections to target-name are made from all devices present in the iSCSI initiator configuration. discovery-address or portal-address is the address through which the target became visible to the initiator.
```

```bash
iscsi target logout target-name { discovery-address | portal-address }
Logout from connections to target-name from the iSCSI initiator. discovery-address or portal-address is the address through which the target became visible to the initiator. A target once logged out by the iSCSI initiator will not be logged in to until iscsi target login is requested.
```

```bash
iscsi target rescan target-name
Rescan target target-name for new LUNs.
```
iscsi target attr showdefault
   Show the default value for target attributes.
iscsi target attr showall
   Show the value of target attributes for all the known targets.
iscsi target attr show target-name
   Show the value of target attributes for target target-name
iscsi target attr setdefault attribute value
   Set the default value of attribute to value. Default value is inherited by any new targets that get added.
iscsi target attr setall attribute value
   Set the value of attribute to value for all the known targets. This does not change the default value as shown in iscsi target attr showdefault. Changes to the values are effective after re-login.
iscsi target attr set target-name attribute value
   Set the value of attribute to value for target-name. Changes to the values are effective after re-login.
iscsi target list
   List the targets visible to the iSCSI initiator. A target can be in any one of ONLINE, OFFLINE, or RETRY states.
iscsi target listdetail target-name
   List detailed information about the target target-name.
iscsi initiatorname setprefix initiatorname-prefix
   Set the prefix used to generate initiator names. Initiator names are generated as initiatorname-prefix followed by the node number of the node.
iscsi initiatorname list
   List the initiator names for all the nodes in the cluster.
quota fs enable fs_name [userquota|groupquota]
quota cifshomedir enable [userquota|groupquota]
   Enable user or group quota on a file system or CIFS home directories.
quota fs disable fs_name [userquota|groupquota]
quota cifshomedir disable [userquota|groupquota]
   Disable user or group quota on a file system or CIFS home directories.
quota fs status fs_name [userquota|groupquota]
quota cifshomedir status [userquota|groupquota]
   Show the status of quota settings on a file system or CIFS home directories. Quota setting status only shows if the quota is enabled or disabled.
quota fs set userquota | groupquota user_or_group_names domain_name
   hardlimit 'softlimit [numinodes|numspace] value [fs_name]
quota cifshomedir set userquota | groupquota user_or_group_names domain_name
   [hardlimit 'softlimit [numinodes|numspace] value]
Set quota value for the users or groups on a file system or CIFS home directories. If \texttt{value} is not specified, then the default value set from the respective \texttt{setdefault} commands is used to configure the quota limit. If \texttt{value} is 0, it is treated as unlimited quota. If all values of user or group quota are 0, the user or group are automatically deleted from the quota settings, which means \texttt{quota fs status} does not show this user’s or group’s settings as all quota values are unlimited for it.

\begin{verbatim}
quota fs setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota cifshomedir setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value]
\end{verbatim}

Set quota value for all the users and groups for whom the quota has already been set with \texttt{set} commands. Other users and groups (for whom quota has not been set previously) are not affected. If \texttt{value} is not specified, then the default value set from the respective \texttt{setdefault} commands is used to configure the quota limit. If \texttt{value} is 0, it is treated as an unlimited quota. If all values of user or group quota are 0, the user or group are automatically deleted from the quota settings, which means \texttt{quota fs status} does not show this user’s or group’s settings, as all quota values are unlimited for it.

\begin{verbatim}
quota fs setbygroup group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
\end{verbatim}

Set the user quota for users of specified groups.

\begin{verbatim}
quota fs show [fs_name] [userquota | groupquota] [user_or_group_names] [domain_name]
quota cifshomedir show [userquota | groupquota] [user_or_group_names] [domain_name]
quota cifshomedir showdetail [userquota | groupquota] [user_or_group_names] [domain_name]
\end{verbatim}

Show the quota values that are already set. This also shows the consumed (used space) quota of the users and groups. \texttt{cifshomedir show} shows the general quota values on the CIFS home directories. \texttt{cifshomedir showdetail} shows the detailed quota values set on each file system for CIFS home directories.

\begin{verbatim}
quota fs setdefault userquota`|``groupquota hardlimit | softlimit numinodes | numspace [value] [fs_name]
quota cifshomedir setdefault userquota | groupquota hardlimit | softlimit numinodes | numspace [value]
\end{verbatim}

Set the default value that is used for the quota limits. The values are stored in the configuration file only. The actual application of quota can be done with \texttt{set} and \texttt{setall} commands using these default values.

\begin{verbatim}
quota fs showdefault [fs_name] [userquota | groupquota]
quota fs showdefault [userquota | groupquota]
\end{verbatim}

Show the default quota values from the configuration file.

\texttt{dedup enable \textit{fs_name} \textit{blksize}}

Enable deduplication on a file system. Deduplication must be enabled for a file system before setting its configuration parameters and schedule. This command also re-enables a deduplication schedule for a file system. \textit{blksize} should be specified in bytes e.g. 4096. It should be the power of 2, multiple of file system’s block size and equal to or less than 128 K. Default block size is 0, which means that if file system’s block size is less than 4096 bytes, then the dedup block size is set to 4096 bytes. Otherwise the dedup block size is set the same as the file system’s block size.

\texttt{dedup disable \textit{fs_name}}
Disable deduplication schedule on a file system. Other information like configuration, schedule, and deduplication database remains intact. **Warning:** keeping deduplication disabled for longer periods of time may reduce the effectiveness of deduplication when it is re-enabled.

```
dedup list [fs_name]
```

List the deduplication configured file systems along with its granularity, state, schedule, and node list where it runs. Currently, node list is picked up automatically by the system and cannot be set by the user.

```
dedup start fs_name [node_name]
```

Start deduplication manually. `fs_name` must be enabled for deduplication to start. You can specify the node to run the deduplication.

```
dedup stop fs_name
```

Stop the deduplication process running on a file system.

```
dedup status [fs_name]
```

Display the current status of deduplication. It shows the file system name, saving amount, status, node where deduplication is either running or has completed, deduplication type i.e., SCHEDULED or MANUAL and other details.

```
dedup set cpu cpuvvalue [fs_name]
```

Set the CPU limit. This parameter can be set as global and/or local. Possible cpuvvalue are `idle` and `yield`.

```
dedup set memory memvalue
```

Set the memory limit in MB. It should be in range 128-4096 MB, default value is 128 MB. This can be set only as a global parameter.

```
dedup set priority priorityval [fs_name]
```

Set priority for deduplication-enabled file system(s). This parameter can be set as global and/or local. Possible priorityval are `low`, `normal`, and `high`.

```
dedup schedule set fs_name hours day [freq]
```

Set schedule for deduplication-enabled file system. This can be set only as a local parameter. Two categories of schedule are allowed i.e., run periodicity and type periodicity. The granularity of schedule is limited to time of day and day of month. `hours` can be specified as * (every hour), /N (every N hours) where N is in range [1-12] or 5 comma-separated hours list in the range [0-23]. *day can be specified as * (every day), /N (every N days), where N is in range [1-15] or any number in the range [1-7], where 1 means Sunday, 2 means Monday, and so on. *freq can be specified in the range 1-5. Default value is 1. A value of 4 means every 4th run deduplicates the file system, whereas the other runs consolidate the changes.

```
dedup schedule modify fs_name hours day [freq]
```

Modify the deduplication schedule set above. `hours`, `day`, and `freq` values can be specified same as above mentioned in `dedup schedule set` command.

```
dedup schedule delete fs_name
```

Delete the deduplication schedule.

```
dedup dryrun fs_name [threshold]
```

Initiate a deduplication dry run on the file system `fs_name`. This reports the approximate saving of space. Dry run can be converted to the actual deduplication if it meets the threshold value.

```
dedup remove fs_name
```

---

**16.1. storage**
Remove deduplication-configuration related information from the specified file systems `fs_name`. This command removes all configurations and the database specific to that file system. Warning: This operation cannot be undone and re-running deduplication may take significant time.

```
compress file fs_name {file|dir} <res_level> [alg_strength] [file_pattern]
```

Compress named file or directory using specified `<res_level>` and `alg_strength`. The default alg-strength is 6. If a directory is specified, then all the files under the named directory are compressed. For directories, you can specify file name patterns. The `<res_level>` can be low, medium, or high.

```
compress list fs_name {file|dir}
```

List compression details for the named file or directory.

```
uncompress file fs_name {file|dir} <res_level>
```

Uncompress the named file or directory using specified `<res_level>`.

```
compress modage create fs_name age_rule
```

Add an age-based rule for scheduled compression jobs for the file system with name `fs_name`. The `age_rule` is specified in days.

```
compress modage remove fs_name
```

Remove the age-based rule for the `fs_name` file system.

```
compress pattern create fs_name pattern_rule
```

Add a pattern-based rule for scheduled-compression jobs for the file system with name `fs_name`.

```
compress pattern remove fs_name
```

Remove the pattern-based rule for the `fs_name` file system.

```
compress schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]
```

Create a compression schedule by name `sched_name`. The time and frequency of this schedule are specified using the command line in crontab format. This scheduled job runs on the node specified by `[node]`. If this node is not online at the time of the job, then this particular compression job runs on the CFS primary.

```
compress schedule remove sched_name
```

Remove the compression schedule by name `sched_name`. Make sure none of the file systems have this `sched_name` assigned.

```
compress schedule show [sched_name]
```

Show the compression schedule information for the schedule by name `sched_name`. If `sched_name` is not specified, then information about all the schedules are displayed.

```
compress schedule start fs_name sched_name res_level [alg_strength]
```

Assign or start the compression schedule by name `sched_name` for the file system by name `fs_name`. The compression job uses resource and algorithm strength specified in args.

```
compress schedule stop fs_name
```

Stop the scheduled compression schedule for the file system by name `fs_name`

```
compress schedule list fs_name
```

List the scheduled compression job details for the file system by name `fs_name`.

```
fs defrag schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]
```

Chapter 16. Storage Commands
Creates a defrag schedule. The time and frequency of this schedule are specified in the command line in cron tab format. This scheduled job runs on the node specified. If this node is not online at the time of the job, then this particular defrag job runs on the CFS primary. The scheduled defrag job may last up to the specified duration hours or minutes.

```
fs defrag schedule remove sched_name
```

Remove the defrag schedule by name sched_name. Make sure none of the file systems have this sched_name assigned.

```
fs defrag schedule show [sched_name]
```

Show the defrag schedule information for the schedule by name sched_name. If sched_name is not specified, then information about all the schedules are displayed.

```
fs defrag schedule start fs_name sched_name
```

Assign or start the defrag schedule by name sched_name for the file system by name fs_name.

```
fs defrag schedule stop fs_name
```

Stop the scheduled defrag schedule for the file system by name fs_name.

```
fs defrag schedule list fs_name
```

List the scheduled defrag job details for the file system by name fs_name.

```
fs policy add operation=move policy_name fs_name from_tier to_tier retrieval_option=Expedited|Standard|Bulk pattern [atime condition] [mtime condition]
```

Create a data movement policy for the scale-out file system fs_name. The policy moves files and directories that meet the criteria from the source tier (from_tier) to the destination tier (to_tier). Movement can be from the cloud tier to a disk tier or from a disk tier to the cloud tier. The retrieval option determines the time needed to move files from Amazon Glacier to on-premises. This option is not used when moving files from on-premises to Amazon Glacier. Expedited retrievals typically complete within 1-5 minutes. The expedited option is expensive and you should use it conservatively. Files moved from the Amazon Glacier tier with the expedited option might return with the following error: InsufficientCapacityException (503 service unavailable). This error occurs if there is insufficient capacity to process the expedited request.

**This error only applies to expedited retrievals and not to standard or bulk retrievals.** Standard retrievals typically complete within 3-5 hours. Bulk retrievals typically complete within 5-12 hours. Bulk is the default option. **Note:** The maximum file size for moving files to AWS Glacier is 4 GB. Pattern identifies the files or directories that you want to move between tiers. Pattern is required. You can further restrict the files or directories to move by specifying the last accessed time (atime) or the last modified time (mtime). The atime and mtime criteria are optional.

```
fs policy add operation=delete policy_name fs_name from_tier pattern [atime condition] [mtime condition]
```

Create a data deletion policy for the scale-out file system fs_name. The policy deletes files and directories that meet the criteria from the specified tier (from_tier). Pattern identifies the files or directories that you want to delete. Pattern is required. You can further restrict the files or directories to delete by specifying the last accessed time (atime) or the last modified time (mtime). The atime and mtime criteria are optional.

```
fs policy modify policy_name pattern [atime condition] [mtime condition]
```

Modify the pattern, atime, and mtime search criteria for the file movement or deletion of the policy. atime and mtime are optional criteria. You cannot change the policy operation or change the storage tiers that were specified when the policy was created.

```
fs policy delete policy_name fs_name
```
Stop any data movement or data deletion policy that was set for a file system. You cannot delete a policy if the policy is running.

**fs policy rename old_policy_name new_policy_name**

Rename an existing policy to a new policy name. You cannot rename a policy if the policy is running.

**fs policy list [fs_name]**

List all the data movement and data deletion policies that are set for all the file systems. If *fs_name* is included in the command, then the command lists all the policies for the specified file system.

**fs policy run policy_name**

Move or prune files according to the configured file system policy *policy_name*. The policy runs in the background until it completes, or until you abort or pause the policy. File system policies are configured only for scale-out file systems (largefs type). The policy runs on the node on which the scale-out file system is active. If a policy run encounters an error, it is retried 5 times before the run is aborted. If the policy is already active but paused, you are prompted whether you want to resume the paused job or to start a new run. You cannot run a policy that is already running, because of a schedule or a previous *fs policy run* command. You also cannot run a policy if a *tier move* command is running for the same path or file system.

**fs policy dryrun policy_name**

Perform a dry run of the file system policy *policy_name*. This command previews the running of the policy, but does not actually move or prune any files. Use this command to estimate the I/O activity involved if the policy is run. The dry run collects the statistics, such as the number of files and the amount of data that will be moved. You cannot perform a dry run if the policy is already running, or if a *tier move* command is running on the same path or file system.

**fs policy status policy_name**

Show the status of the currently running policy or dry run of the policy *policy_name*. If the policy is not currently running, the status shows the most recent run. The information includes the type of the run (normal or dry run), the status, the total data, the amount of data moved so far, the number of files, the number of files moved or deleted so far, and the name of the last file completed by the policy run.

**fs policy abort policy_name**

Abort the currently executing policy run or dry run for the policy *policy_name*. The abort is immediate and interrupts any data movement in progress. The aborted policy cannot be resumed using the *fs policy resume* command. If you need to restart the policy, start a new run with the *fs policy run* command.

**fs policy pause policy_name**

Pause the currently executing policy run or dry run for the policy *policy_name*. The pause is immediate and interrupts any data movement in progress. You can resume the policy using the *fs policy resume* command. You can abort the paused policy using the *fs policy abort* command. When you pause a policy, the scheduled runs of the policy are also skipped until the policy is resumed.

**fs policy resume policy_name**

Restarts the policy run or dry run that was paused with the *fs policy pause* command. The policy resumes from the point where the policy run was interrupted.

**fs policy schedule create fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]**

Create the file system policy schedule for the file system *fs_name*. The schedule uses a time format similar to the format used in UNIX cron configuration files. The schedule applies to the file system policies created using the *fs policy create* command. When a schedule is set for a particular file system, all the policies for that file system are started at the scheduled times. If any policy is paused using
the \texttt{fs policy pause} command, the policy does not run at the scheduled time. The policy is skipped until the policy is resumed using the \texttt{fs policy resume} command.

\textbf{About the schedule format:}

A schedule is specified in a format similar to the UNIX crontab format. The format uses five fields to specify when the schedule runs:

- \textbf{minute} Enter a numeric value between 0-59, or an asterisk (*), which represents every minute. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- \textbf{hour} Enter a numeric value between 0-23, or an asterisk (*), which represents every hour. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- \textbf{day\textunderscore of\textunderscore the\textunderscore month} Enter a numeric value between 1-31, or an asterisk (*), which represents every day of the month. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- \textbf{month} Enter a numeric value between 1-12, or an asterisk (*), which represents every month. You can also use the names of the month. Enter the first three letters of the month (you must use lowercase letters). You can also enter a step value (*/x), or a range.

- \textbf{day\textunderscore of\textunderscore the\textunderscore week} Enter a numeric value between 0-6, where 0 represents Sunday, or an asterisk (*), which represents every day of the week.

You can also enter the first three letters of the week (you must use lowercase letters). You can also enter a step value (*/x), or a range.

A step value (*/x) specifies that the schedule runs at an interval of x. The interval should be an even multiple of the field’s range. For example, you could specify */4 for the hour field to specify every four hours, since 24 is evenly divisible by 4. However, if you specify */15, you may get undesired results, since 24 is not evenly divisible by 15. The schedule would run after 15 hours, then 7 hours.

A range of numbers (two values separated by a hyphen) represents a time period during which you want the schedule to run.

Examples:

- To run the schedule every two hours every day: 0 */2 * * *
- To run the schedule on 2:00 a.m. every Monday: * 2 * * 1
- To run the schedule at 11:15 p.m. every Saturday: 15 23 * * 6

\texttt{fs policy schedule modify fs\_name [minute] [hour] [day\textunderscore of\textunderscore the\textunderscore month] [month] [day\textunderscore of\textunderscore the\textunderscore week]}

Modifies the file system policy schedule for the file system \texttt{fs\_name}. The schedule uses a time format similar to the format used in UNIX cron configuration files. Refer to the \texttt{fs policy schedule create} section for the detailed description of the schedule format.

\texttt{fs policy schedule remove fs\_name} Removes the file system policy schedule associated with the file system \texttt{fs\_name}.

\texttt{fs policy schedule list fs\_name} Lists the file system policy schedule associated with the file system \texttt{fs\_name}.

\texttt{fs retention set path rtime} Sets the retention on a file path \texttt{path} or on all the files that are currently present in specified path \texttt{path}. \texttt{rtime} can be in [1-9](d|D|m|M|y|Y) or mm-dd-yyyy format.

\texttt{fs retention show path} Shows the retention value applied on the specified file path \texttt{path}.

\texttt{fs retention clear path} Clears the retention on a file path \texttt{path} or on all the files that are currently present in specified path \texttt{path}.

\texttt{fs worm set fs\_name} Enable worm support for the specified file system.
fs worm clear fs_name  Disable worm support for the specified file system.

16.1.4 EXAMPLES

Display list of disks in tabular form.

```
Storage> disk list stats
Disk nasgw9_2 nasgw9_1 nasgw9_3 nasgw9_4 nasgw9_5 nasgw9_6
===== ======= ======= ======= ======= ======= =======
AMS_WMS0_0 OK OK OK OK OK OK
AMS_WMS0_1 OK OK OK OK OK OK
DS4800-0_0 OK OK OK OK OK OK
DS4800-0_1 OK OK OK OK OK OK
nasgw9_2_Disk_0 OK NOT_CONN NOT_CONN NOT_CONN NOT_CONN NOT_CONN
nasgw9_1_Disk_1 OK OK OK OK OK OK
EMC_CLARiiON0_0 OK OK OK OK OK OK
EMC_CLARiiON0_1 OK OK OK OK OK OK
```

Display the list of disks and their properties.

```
Storage> disk list detail
Disk Pool Enclosure Array Type Size (Use%) Transport ID Serial Number
---- ============== ========== =========== ============ ==========  
ams_wms0_10 *coordinator* ams_wms0 A/A 1.00G 0.0% FC  
---HITACHI:DF600F:4:1 71011588000A  
ams_wms0_11 *coordinator* ams_wms0 A/A 1.00G 0.0% FC  
---HITACHI:DF600F:4:2 71011588000B  
ams_wms0_12 p03 ams_wms0 A/A 1.00G 27.5% FC  
---HITACHI:DF600F:4:3 71011588000C  
ams_wms0_13 p03 ams_wms0 A/A 1.00G 18.8% FC  
---HITACHI:DF600F:4:4 71011588000D  
ams_wms0_14 p04 ams_wms0 A/A 1.00G 17.8% FC  
---HITACHI:DF600F:4:5 71011588000E  
```

Show the list of multiple paths of disks connected to all the nodes of the cluster. Also show the status of those paths on each node in the cluster.

```
Storage> disk list paths
Disk Paths nasgw78_2 nasgw78_1
---- ----- ======= =======
AMS_WMS0_0 Path 1 primary,enabled,active primary,enabled,active
AMS_WMS0_1 Path 1 primary,enabled,active primary,enabled,active
nasgw78_2_Disk_0 Path 1 enabled,active -
nasgw78_1_Disk_1 Path 1 - enabled,active
```

Grow a selected disk.

```
Storage> disk grow Disk_0
ACCESS disk SUCCESS V-288-0 disk grow Disk_0 completed successfully.
```

Format a specified disk.

```
Storage> disk format aluadisk0_7
You may lose all the data on the disk, do you want to continue (y/n, the default is n): y
```
Remove a disk from the configuration.

Storage> disk remove aluadisk0_7
Removed disk emc0_03ff from nasgw78_1
Removed disk emc0_03ff from nasgw78_2

Destroy the coordinator pool.

Storage> disk format aluadisk0_7, aluadisk0_8
You may lose all the data on the disk, do you want to continue (y/n, the default is _→n):y
ACCESS Disk SUCCESS V-288-0 disk format: aluadisk0_7 has been formatted successfully.

ACCESS Disk ERROR V-288-0 Disk aluadisk0_8 has invalid pool configuration. Format _→with force option to clean up else run scanbus to retrieve.
Storage> disk format aluadisk0_8 force
You may lose all the data on the disk, do you want to continue (y/n, the default is _→n):y
ACCESS Disk SUCCESS V-288-0 disk format: aluadisk0_8 has been formatted successfully.

Enable I/O fencing on the disks ams_wms0_000d, ams_wms0_000e, ams_wms0_000f (only three disks required).

Storage> fencing on disk ams_wms0_000d,ams_wms0_000e,ams_wms0_000f
ACCESS fencing Success V-288-0 IO Fencing feature now Enabled with SCSI3 Persistent _→Reservations
100% [#] Enabling fencing

Check I/O fencing status after enabling fencing.

Storage> fencing status

IO Fencing Status
=================
Enabled
Disk Name       Coord Flag On
--------------   ------------
amwms0_000d    Yes
ams_wms0_000e  Yes
ams_wms0_000f  Yes

Disable I/O fencing on all the nodes.

Storage> fencing off
ACCESS fencing Success V-288-0 IO Fencing feature now Disabled
100% [#] Disabling fencing

Check I/O fencing status after disabling I/O fencing.
Replace `ams_wms0_000f` with `ams_wms0_000c` with fencing in Enabled mode.

Replace `ams_wms0_000f` with `ams_wms0_000c` with fencing in Disabled mode.

Check I/O fencing status after the I/O fencing replace operation is completed.

Enable I/O fencing on all of the nodes without specifying the disks. This will work only if the user had specified three disks earlier for I/O fencing.

Check I/O fencing status after enabling I/O fencing again.

Create a mirrored file system with name `fs1` with disks from the pools `pool1` and `pool2`.

---

**Storage> fencing status**

**IO Fencing Status**

*Disabled*

<table>
<thead>
<tr>
<th>Disk Name</th>
<th>Coord</th>
<th>Flag</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>amswms0_000d</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>amswms0_000e</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>amswms0_000f</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Replace `ams_wms0_000f` with `ams_wms0_000c` with fencing in Enabled mode.

Replace `ams_wms0_000f` with `ams_wms0_000c` with fencing in Disabled mode.

Check I/O fencing status after the I/O fencing replace operation is completed.

Enable I/O fencing on all of the nodes without specifying the disks. This will work only if the user had specified three disks earlier for I/O fencing.

Check I/O fencing status after enabling I/O fencing again.

Create a mirrored file system with name `fs1` with disks from the pools `pool1` and `pool2`.
Storage> fs create mirrored fs1 100M 2 pool1,pool2
100% [#] Creating mirrored filesystem

Defragment a file system now.
Storage> storage fs defrag now fs_t 2M
Do you want to continue? yes|no
yes

You can check defrag status by running fs list command
Storage> storage fs list fs_t
General Info:
===============
Block Size: 8192 Bytes
Version: Version 10
phoenix_01: online
phoenix_02: online

Primary Tier
============
Size: 100.00M
Use%: 6%
Layout: simple
Mirrors: -
Columns: -
Stripe Unit: 0.00 K
Meta Data: metaOk
FastResync: Disabled

1. Mirror 01:
List of pools: pool1
List of disks: vmdk0_4

FS Type: Normal

Defrag Status: Done successfully
Fullfsck Status: Not Running
Resync Status: Not Running
Rollsync Status: Not Running
Relayout Status: Not Running

Create a file system for a virtual machine workload with 4 striped columns.
Storage> fs create pretuned vmdk_fs 100g pool1 workload=virtualmachine
      →layout=striped 4

Create a file system for a media server workload with 8 striped columns.
Storage> fs create pretuned media_fs 100g pool2 workload=mediaserver layout=striped-
      →mirror 8

List the file system properties of vmdk_fs.
Storage> fs list vmdk_fs
General Info:
===============
Block Size: 8192 Bytes
Add a mirror to file system fs1.

```
Storage> fs addmirror fs1 pool3,pool4
```

Remove a mirror of file system fs1 that is residing on Disk AMS_WMS0_0.

```
Storage> fs rmmirror fs1 AMS_WMS0_0
```

Add two columns to file system fs1.

```
Storage> fs addcolumn fs1 2 pool3
```

Remove column from file system fs1.

```
Storage> fs rmcolumn fs1
```

Show file systems that have stale mirrors.

```
Storage> fs checkmirror
fs_name:
--
mirror3
```

Resynchronize all stale mirrors for all file systems.

```
Storage> fs resync
Resync stale mirror for file systems are started in background.
```

Show resynchronization progress running in background.

```
Storage> fs checkresync
FS MIRROR TYPE PROGRESS START_TIME
---USED_TIME REMAINING_TIME
---------------------------------------------------------------
mir2 tier 1,mirror 02 RESYNC 6.46% Jun/05/2011/09:39:53
0:5:9 1:14:34
```
Make a file system offline.

Storage> fs offline fs1
100% [#] Offline filesystem

Check and repair a file system while it is in offline state.

Storage> fs fsck fs1

Make a file system online.

Storage> fs online fs1
100% [#] Online filesystem

Check and repair a file system while it is in offline state.

Storage> fs fsck fs1
ACCESS fs ERROR V-288-693 fs1 must be offline to perform fsck.

Grow file system’s primary tier size to 1 G.

Storage> fs growto primary fs1 1g

Grow file system’s primary tier size by 50 M.

Storage> fs growby primary fs1 50M

Shrink file system’s primary tier by the specified size.

Storage> fs shrinkby primary fs1 10m

Shrink file system’s primary tier to just 50 M.

Storage> fs shrinkto primary fs1 50M

View the list of file systems.

Storage> fs list

<table>
<thead>
<tr>
<th>FS</th>
<th>STATUS</th>
<th>SIZE</th>
<th>LAYOUT</th>
<th>MIRRORS</th>
<th>COLUMNS</th>
<th>USE%</th>
</tr>
</thead>
<tbody>
<tr>
<td>fsl</td>
<td>online</td>
<td>100.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>fs2</td>
<td>online</td>
<td>100.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>3%</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>fs3</td>
<td>online</td>
<td>700.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>fs4</td>
<td>online</td>
<td>69.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>4%</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
<tr>
<td>fs5</td>
<td>online</td>
<td>1.94G</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>1%</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
<td>no</td>
<td>no</td>
<td></td>
</tr>
</tbody>
</table>
Display detailed information for a specific file system.

```
Storage> fs list mir4
General Info:
===============
Block Size: 1024 Bytes
Version: Version 8
Cluster5_01: online

Primary Tier
============
Size: 30.00G
Use%: 0%
Layout: mirrored
Mirrors: 4
Columns: -
Stripe Unit: 0.00 K
FastResync: Enabled

1. Mirror 01:
   List of pools: pool1
   List of disks: disk1 disk2

2. Mirror 02:
   List of pools: pool1
   List of disks: disk3 disk4

3. Mirror 03:
   List of pools: pool1
   List of disks: disk5 disk6

4. Mirror 04:
   List of pools: pool1
   List of disks: disk7 disk8

Secondary Tier
==============
Size: 20.00G
Use%: 0%
Layout: mirrored
Mirrors: 2
Columns: -
Stripe Unit: 0.00 K
FastResync: Disabled

1. Mirror 01:
   List of pools: pool1
   List of disks: disk9 disk10

2. Mirror 02:
   List of pools: pool1
   List of disks: disk11 disk12

FS Type: Normal
Defrag Status: Not Running
Fullfsck Status: Not Running
Resync Status:
   Tier 1, Mirror 03: 7.67%  Start_time: Jun/05/2011/15:10:26  Work_time: 0:1:14
   Remaining_time: 14:50
```
Disability FastResync for a file system.

Storage> fs unsetfastresync fs6

Try disabling FastResync for a file system where it is already in the disabled state.

Storage> fs unsetfastresync fs6
ACCESS fs ERROR V-288-655 Fastresync is not enabled for fs6.

Enable FastResync for a file system.

Storage> fs setfastresync fs6

Try enabling FastResync for a file system where it is already in the enabled state.

Storage> fs setfastresync fs6
ACCESS fs ERROR V-288-651 File system fs6 is already fastresync enabled.

Destroy a file system.

Storage> fs destroy fs6
100% [#] Destroy filesystem
FS ============
fs1

Display WWN information for a particular node

Storage> hba democluster_01
Node Host Initiator HBA WWNs
==== ============================
democluster_01 21:00:00:1b:32:1e:5c:ba, 21:01:00:1b:32:3e:5c:ba

Display WWN information for all the running nodes in the cluster

Storage> hba
Node Host Initiator HBA WWNs
==== ============================
democluster_01 21:00:00:1b:32:1e:5c:ba, 21:01:00:1b:32:3e:5c:ba
democluster_02 21:00:00:e0:8b:92:53:d7, 21:01:00:e0:8b:b2:53:d7

Create a pool pool1 with disks Disk_0,Disk_1.

Storage> pool create pool1 Disk_0,Disk_1 isolated=yes
ACCESS pool Success V-288-1015 Pool pool1 created successfully.
100% [#] Creating pool pool1

View the list of pools.
Storage> pool list
Pool  Pool Type  List of disks
===== ======== ============== 
pool1 Isolated  Disk_0 Disk_1
pool2 Normal   Disk_2 Disk_5

Destroy pool pool1.
Storage> pool destroy pool1
ACCESS pool SUCCESS V-288-2056 successfully destroyed the pool.

Remove disks from a pool.
Storage> pool rmdisk Disk_2
ACCESS pool Success V-288-1360 Disk(s) Disk_2 have been removed successfully.

Add disk Disk_2 to pool pool2.
Storage> pool adddisk pool2 Disk_2
ACCESS pool Success V-288-1001 Disk(s) Disk_2 are added to pool2 successfully.

Rename pool1 to p01.
Storage> pool rename pool1 p01
ACCESS pool Success V-288-1017 Pool rename successful.

Move disk Disk_0 from pool p01 to pool pool2.
Storage> pool mvdisk p01 pool2 Disk_0
ACCESS pool Success V-288-1002 Disk(s) moved successfully.

View the free space in each of the pools.
Storage> pool free
Pool Free Space Total Space Use%
===== =========== =========== ====
p01 989.64M 989.64M 0%
pool2 2.90G 2.90G 0%

View the free space in pool2.
Storage> pool free pool2
Disk Free Space Total Space Use%
==== =========== =========== ====
Disk_0 989.64M 989.64M 0%
Disk_2 991.69M 991.69M 0%
Disk_5 991.69M 991.69M 0%

Mark disk Disk_2 in pool2 as spare disk.
Storage> pool markdiskspare pool2 Disk_2
ACCESS Pool SUCCESS V-288-1360 Disk(s) Disk_2 have been marked as spared disks successfully.

Remove spare disk flag on Disk_2 in pool2.
Scan SCSI bus for newly added disks.

Storage> scanbus
100% [#] Scanning the bus for disks

Create a snapshot of a file system.

Storage> snapshot create snapshot1 fs1
100% [#] Create snapshot

Restore a file system by a given snapshot.

Storage> snapshot restore fs0 snap00

Destroy a snapshot of an existing file system.

Storage> snapshot destroy snap1 fs1
100% [#] Destroy snapshot

View the list of snapshots.

Storage> snapshot list

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>FS</th>
<th>Status</th>
<th>ctime</th>
</tr>
</thead>
<tbody>
<tr>
<td>snap2</td>
<td>fs1</td>
<td>offline</td>
<td>2009.Jul.27.02:40:43</td>
</tr>
<tr>
<td>sc1_24_Jul_2009_21_34_01_IST</td>
<td>fs1</td>
<td>offline</td>
<td>2009.Jul.24.21:34:03</td>
</tr>
<tr>
<td>presnap_sc1_24_Jul_2009_18_34_02_IST</td>
<td>fs1</td>
<td>offline</td>
<td>2009.Jul.24.18:34:04</td>
</tr>
<tr>
<td>sc1_24_Jul_2009_17_34_02_IST</td>
<td>fs1</td>
<td>offline</td>
<td>2009.Jul.24.17:34:04</td>
</tr>
</tbody>
</table>

Display the list of snapshots for a given file system.

Storage> snapshot list fs2

<table>
<thead>
<tr>
<th>Snapshot</th>
<th>Schedule Name</th>
<th>Status</th>
<th>ctime</th>
</tr>
</thead>
<tbody>
<tr>
<td>snap2</td>
<td></td>
<td>offline</td>
<td>2009.Jul.27.02:40:43</td>
</tr>
<tr>
<td>presnap_sc1_24_Jul_2009_18_34_02_IST</td>
<td></td>
<td>offline</td>
<td>2009.Jul.24.18:34:04</td>
</tr>
</tbody>
</table>

16.1. storage 283
Display the list of snapshots corresponding to a file system and schedule name.

```
Storage> snapshot list fs1 scl
Snapshot                  Status   ctime            mtime
removable
```

Make a snapshot offline.

```
Storage> snapshot offline snapshot1 fs1
100% [#] Offline snapshot
```

Make a snapshot online.

```
Storage> snapshot online snapshot1 fs1
100% [#] Online snapshot
```

Enable the snapshot quota of a file system.

```
Storage> snapshot quota on fs1
Storage> snapshot quota on fs1 1M
```

Disable the snapshot quota of a file system.

```
Storage> snapshot quota off fs2
Storage> snapshot quota off fs3
Storage> snapshot quota off fs4
Storage> snapshot quota off fs5
```

Display the list of snapshot quotas of all the file systems.

```
Storage> snapshot quota list
FS ----------- Quota Capacity Limit
fs1 ----------------- on 1M
fs2 -------------- off 0
fs3 ----------- off 0
fs4 ----------- off 0
fs5 ----------- off 0
```

Create a schedule for automated snapshot creation of a given file system every 3 hours on a daily basis without any restrictions on the maximum number of snapshots.
Modify the existing schedule so that the snapshot is created every 2 hours on the first day of the week and only 20 snapshots can be created for a given schedule.

Storage> snapshot schedule modify schedule1 fs1 20 * 2 * * 1

Destroy all automated snapshots created under a given schedule and file system.

Storage> snapshot schedule destroyall schedule1 fs1

Preserve a snapshot created according to a given schedule and file system name.

Storage> snapshot schedule preserve schedule1 fs1 schedule1_Feb_27_16_42_00_IST

List all schedules created for automated snapshot creation corresponding to an existing file system.

Storage> snapshot schedule show fs3

<table>
<thead>
<tr>
<th>FS</th>
<th>Schedule Name</th>
<th>Max Snapshot</th>
<th>Minute</th>
<th>Hour</th>
<th>Day</th>
<th>Month</th>
<th>WeekDay</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs3</td>
<td>sched1</td>
<td>0</td>
<td>*/2</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>fs3</td>
<td>sched2</td>
<td>20</td>
<td>*/45</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

List automated snapshot schedules for all the file systems.

Storage> snapshot schedule show

<table>
<thead>
<tr>
<th>FS</th>
<th>Schedule Name</th>
<th>Max Snapshot</th>
<th>Minute</th>
<th>Hour</th>
<th>Day</th>
<th>Month</th>
<th>WeekDay</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs6</td>
<td>sc1</td>
<td>10</td>
<td>*/5</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>fs1</td>
<td>sc1</td>
<td>10</td>
<td>*/25</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

Delete all schedules created for automated snapshot creation / removal corresponding to an existing file system.

Storage> snapshot schedule delete fs1

Create a mirrored file system with name fs1 with disks from the pools pool1 and pool2. Add a mirrored tier to this file system.

Storage> fs create mirrored fs1 100M 2 pool1,pool2

Create a simple file system on encrypted volume

Storage> fs create simple fs4 1g pool1 blksize=2048 pdir_enable=no encrypt=on

Create a mirrored file system with name fs4 with disks from the pools pool1 and pool2. Add a mirrored tier to this file system.

Storage> fs create mirrored fs4 100M 2 pool1,pool2

100% [%] Creating mirrored filesystem

Storage> tier add mirrored fs4 100M 2 pool3,pool4

100% [%] Creating mirrored secondary tier of filesystem

Create a simple file system on encrypted volume

Storage> fs create simple fs5 1g pool1 blksize=2048 pdir_enable=no encrypt=on

100% [%] Creating simple filesystem

ACCESS fs SUCCESS V-288-0 Created simple file system fs5
Display detailed information for a specific file system

Storage> fs list fs4
General Info:
===============
Block Size: 2048 Bytes
Version: 11
Volume Encrypted: Yes
ISA_01: online
ISA_02: online

Primary Tier
============
Size: 1.00G
Use%: 5%
Layout: simple
Mirrors: -
Columns: -
Stripe Unit: 0.00 K
Meta Data: metaOk
FastResync: Disabled

1. Mirror 01:
List of pools: pool1
List of disks: isa_01_intel_nvme2_0

FS Type: Normal

Defrag Status: Not Running
Fullfsck Status: Not Running
Resync Status: Not Running
Rollsync Status: Not Running
Relayout Status: Not Running

WORM Enabled: No

Create a simple WORM enabled file system

Storage> fs create simple fs1 1G pooll blksize=2048 pdir_enable=no encrypt=off
       worm=yes
100% [#] Creating simple filesystem
ACCESS fs SUCCESS V-288-0 Created simple file system fs1

Display detailed information for a specific file system

Storage> fs list fs1
General Info:
===============
Block Size: 2048 Bytes
Version: 13
Volume Encrypted: No
Max IOPS: 0
ISA_01: online
ISA_02: online

Primary Tier
============
Size: 1.00G
Use%: 5%

Add a new AWS service with name `amzservice`:

```
Storage> cloud addservice amzservice service_provider=AWS
Access_Key: ZTVhY2E3M2JlYWQyNWFk
Secret_Key:
```

Add an S3-compatible cloud service provider with name `isaobj`:

```
Storage> cloud addservice isaobj service_provider=S3_COMPATIBLE
REST Endpoint: s3.isaobj:8143
Access_Key: ZTVhY2E3M2JlYWQyNWFk
Secret_Key: Successfully added new cloud service.
```

Add the cloud storage of the Amazon S3 service, named awstest, in the region of us-west-2 as the cloud tier `cloudtier` for the scale-out file system `largefs1`.

```
Storage> tier add cloud largefs1 cloudtier awstest us-west-2
ACCESS tier SUCCESS V-288-0 Tier cloudtier is added for largefs1
```

Add S3-compatible cloud storage, named `s3comptest`, in the region of `none` as the cloud tier for the scale-out file system `largefs1`. Use `none` as the region for S3-compatible cloud storage.

```
Storage> tier add cloud largefs1 va01 s3comptest none
ACCESS tier SUCCESS V-288-0 Tier va01 is added for largefs1
```

List all the configured cloud services.

```
Storage> cloud listservice
<table>
<thead>
<tr>
<th>Service</th>
<th>Provider</th>
<th>Access Key</th>
<th>REST Endpoint</th>
</tr>
</thead>
<tbody>
<tr>
<td>amzservice</td>
<td>AWS</td>
<td>AKIA----B4WA</td>
<td>-</td>
</tr>
<tr>
<td>isaobj</td>
<td>S3_COMPATIBLE</td>
<td>ZTVh----NWFk</td>
<td>s3.isaA:8143</td>
</tr>
</tbody>
</table>
```

Remove an existing cloud service named `amzservice`:
Storage> cloud removeservice amzservice

Remove an existing cloud service named isaobj:

Storage> cloud removeservice isaobj

Add a mirror to the secondary tier of the file system fs1.

Storage> tier addmirror fs1 pool5
100% [#] Adding mirror to secondary tier of filesystem

Add a column to the tier of the file system.

Storage> tier addcolumn fs1 1 pool1
ACCESS fs INFO V-288-2644 This operation may take some time to complete. You can check the status in storage fs list fsname

Remove a column from the tier of the file system.

Storage> tier rmcolumn fs1
ACCESS fs INFO V-288-2711 Only one column will be removed.
ACCESS fs INFO V-288-2644 This operation may take some time to complete. You can check the status in storage fs list fsname

Show list of files on the primary tier of file system fs1.

Storage> tier listfiles fs1 primary
/.placement_policy.xml
/lost+found/changelog

Show list of files on the secondary tier of file system fs1.

Storage> tier listfiles fs1 secondary

Show tier location of file a.txt, which is in the root directory of file system fs1.

Storage> tier mapfile fs1 /a.txt
Tier Extent Type File Offset Extent Size
==== =========== =========== ===========
Primary Data 0 Bytes 1.00 KB

The following command sets the policy of file system fs1, such that the new files get created on the primary tier. If a file has not been accessed for more than 7 days, then it is moved from the primary to the secondary tier. If the access temperature of the files in the secondary tier is more than 5, then these files are moved from the secondary tier to the primary tier. Access temperature is calculated over a 3-day period. The prune policy is to show the file system can delete the inactive files on the secondary tier after the specified time.

Modify the tier policy.

Storage> tier policy modify fs1 primary 7 5 3
ACCESS fs SUCCESS V-288-0 Successfully modified tiering policy for File system fs1

List the tiering policy for all the file systems.
Modify the prune policy.

```
Storage> tier policy prune modify fs1 180
ACCESS fs SUCCESS V-288-0 Successfully modified the Prune policy for File system fs1
```

List the tiering prune policy for all the file systems.

```
Storage> tier policy prune modify fs1 180
FS Delete After
-------------------------------
fs1 180
```

Run the tiering policy for file system fs1.

```
Storage> tier policy run fs1
ACCESS fs SUCCESS V-288-0 Successfully ran tiering policy for File system fs1
```

Show list of files that will be moved and/or deleted by running the policy.

```
Storage> tier query fs1
/a.txt
/b.txt
/c.txt
/d.txt
```

Set schedule of file system fs1.

```
Storage> tier schedule modify fs1 1 1 1 * *
ACCESS fs SUCCESS V-288-0 Command 'tier schedule modify' executed sucessfully for fs1
```

Get the tiering schedule for all the file systems.

```
Storage> tier schedule list
FS Minute Hour Day Month WeekDay NodeName
------------------------------- -----------
fs1 1 1 1 * * master node
```

Relocate a file from the secondary tier to the primary tier of file system fs1.

```
Storage> tier schedule relocate fs1 /a.txt
ACCESS fs SUCCESS V-288-0 Successfully relocated /a.txt from secondary to primary tier for File system fs1
```

Remove the tiering schedule for file system fs1.

```
Storage> tier schedule remove fs1
ACCESS fs SUCCESS V-288-0 Command tier schedule remove executed sucessfully for fs1
```

Remove the policy of file system fs1.

```
Storage> tier policy remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed tiering policy for File system fs1
```
Remove the prune policy of file system fs1.

```
Storage> tier policy prune remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed the Prune policy for File system fs1
```

Remove a mirror from the secondary tier of file system fs1.

```
Storage> tier rmmirror fs1
```

Remove the cloud tier cloudtier from scale-out file system largefs1.

```
Storage> tier remove largefs1 cloudtier
ACCESS tier SUCCESS V-288-0 Tier cloudtier is removed
```

Set fastresync for the tier of the file system.

```
Storage> tier setfastresync adistr pool1
Storage>
```

Unset fastresync for the tier of the file system.

```
Storage> tier unsetfastresync adistr
ACCESS fs SUCCESS V-288-1817 Disabled fast resync on the file system adistr
```

Show the access statistics of the cloud tier cloudtier.

```
Storage> tier stats show largefs1 cloudtier
GET 168
GET bytes 174.5MB
PUT 918
PUT bytes 10.3GB
DELETE 20
```

Monitor the access statistics of the cloud tier cloudtier every 10 seconds.

```
Storage> tier stats monitor largefs1 cloudtier 10

<table>
<thead>
<tr>
<th>GET</th>
<th>GET bytes</th>
<th>PUT</th>
<th>PUT bytes</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1.4MB</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>3</td>
<td>714.0KB</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

Reset the access statistics of the cloud tier cloudtier to zero. After executing the tier stats reset command, the output for the tier stats show command is reset to zero.

```
Storage> tier stats reset largefs1 cloudtier
```

Show the usage of the cloud tier cloudtier.

```
Storage> tier stats usage largefs1 cloudtier
Storage Utilized 223.1GB
Number of objects 488
Number of files 231
```

Enable deduplication on the file system fs1.

```
Storage> dedup enable fs1 blksize=8192
```
Set the deduplication schedule.

```
Storage> dedup schedule set fs1 0,6,12,18 2 3
```

List deduplication enabled file systems.

```
Storage> dedup list
Default Priority CPU Memory
--------------------------------
NORMAL IDLE 128M
Filesystem Priority CPU Granularity Enabled Schedule
---NodeList
-----------------------------------------------
/vx/fs1 NORMAL IDLE 8192B YES SET
---node_01,node_02
```

Show deduplication parameters details of file system /fs1.

```
Storage> dedup list fs1
Priority NORMAL
CPU IDLE
Memory 128M
Granularity 8192B
Enabled YES
Schedule hours Every hour
Schedule day interval Every Sunday
Schedule frequency 1
NodeList node_01,node_02
```

Check whether dedup dry run reaches to threshold value 60%.

```
Storage> dedup dryrun fs1 60
```

Show deduplication status.

```
Storage> dedup status
Filesystem Saving Status Node Type Details
-----------------------------------------------
/vx/fs1 00% COMPLETED node_01 MANUAL 2011/05/23
17:08:00 Dryrun threshold not met. Cleaning up...
```

Start deduplication on file system /fs1.

```
Storage> dedup start fs1
```

Start deduplication on file system /fs1 at node node_01.

```
Storage> dedup start fs1 node1
```

Show deduplication status.

```
Storage> dedup status
Filesystem Saving Status Node Type Details
-----------------------------------------------
/vx/fs1 -- RUNNING node_01 MANUAL --
```
Show status output after completion of deduplication.

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Saving</th>
<th>Status</th>
<th>Node</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vx/fs1</td>
<td>34%</td>
<td>COMPLETED</td>
<td>node_01</td>
<td>MANUAL</td>
<td>2011/05/23</td>
</tr>
</tbody>
</table>

End detecting duplicates and filesystem changes 0

Remove deduplication on file system fs1.

Storage> dedup remove fs1

List deduplication enabled file system.

Create a data movement policy policy1 for file system fs1 to move the files with file name extensions of .txt and .pdf that were not accessed or modified within the last 2 days from the primary (disk tier) to tier1 (cloud tier).

Storage> fs policy add operation=move policy1 fs1 primary tier1 retrieval_option=Standard \*.txt,\*.pdf atime >2d mtime >2d
ACCESS policy SUCCESS V-288-0 Policy policy1 for fs fs1 added successfully.

Create a data deletion policy policy2 for file system fs1 to delete the files with file name extensions of .txt and .pdf that were not accessed or modified within the last 2 days from tier1 (cloud tier).

Storage> fs policy add operation=delete policy2 fs1 tier1 \*.txt,\*.pdf atime >2d mtime >2d
ACCESS policy SUCCESS V-288-0 Policy policy2 for fs fs1 added successfully.

Modify data movement policy policy1 for file system fs1 to move the files with file name extension of .doc that were not accessed or modified within the last 3 days.

Storage> fs policy modify policy1 \*.doc atime >3d mtime >3d
ACCESS policy SUCCESS V-288-0 Policy policy1 modified successfully.

List all policies.

<table>
<thead>
<tr>
<th>Name</th>
<th>FS name</th>
<th>Action</th>
<th>Source Tier</th>
<th>Destination Tier</th>
<th>Retrieval Option</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>fs1</td>
<td>delete</td>
<td>tier1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>fs2</td>
<td>move</td>
<td>primary</td>
<td>tier1</td>
<td></td>
</tr>
<tr>
<td>policy2</td>
<td>fs1</td>
<td>delete</td>
<td>tier1</td>
<td></td>
<td>Standard</td>
</tr>
<tr>
<td>policy1</td>
<td>fs1</td>
<td>move</td>
<td>primary</td>
<td>tier1</td>
<td>Standard</td>
</tr>
<tr>
<td></td>
<td>fs2</td>
<td>move</td>
<td>primary</td>
<td>tier2</td>
<td></td>
</tr>
<tr>
<td>policy</td>
<td>fs1</td>
<td>move</td>
<td>primary</td>
<td>tier2</td>
<td></td>
</tr>
<tr>
<td>policy2</td>
<td>fs2</td>
<td>delete</td>
<td>tier2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
List all policies set for file system fs1.

```
Storage> fs policy list fs1
Name  FS name  Action  Source Tier  Destination Tier  Retrieval Option  Pattern
-------  --------  -------  -----------  ---------------  ----------------  ================
    policy2 fs1  delete  tier1  Standard  *.
                      >2d  >2d  not running
    policy1 fs1  move    primary tier1  Standard  \
                      >3d  >3d  not running
```

Delete policy policy1 set for file system fs1.

```
Storage> fs policy delete policy1 fs1
ACCESS policy SUCCESS V-288-0 Policy policy1 for fs fs1 deleted successfully.
```

Rename policy2 to policy3.

```
Storage> fs policy rename policy2 policy3
ACCESS policy SUCCESS V-288-0 Policy policy2 renamed to policy3.
```

Show the status of policy run for the policy Policy1.

```
Storage> fs policy status Policy1
Policy Name: Policy1
==================================================
Policy Run Type: normal
Policy Run Status: running
Total Data (Files): 93.1 GB (100000)
Moved/Deleted Data (Files): 47.7 MB (879)
Last File Visited: file100.txt
```

Abort the currently running policy Policy1.

```
Storage> fs policy abort Policy1
ACCESS policy INFO V-288-0 Policy Policy1 aborted successfully.
```

Start a dry run of the policy Policy1.

```
Storage> fs policy dryrun Policy1
ACCESS policy INFO V-288-0 Policy Policy1 dryrun started in background, please check 'fs policy status' for progress.
```

Pause the currently running policy Policy1.

```
Storage> fs policy pause Policy1
ACCESS policy INFO V-288-0 Policy Policy1 paused successfully.
```

Run the currently paused policy Policy1.

```
Storage> fs policy run Policy1
Policy Policy1 is not running currently, as it was killed/paused. Would you like to _
-->start new run (y/n): y
ACCESS policy INFO V-288-0 Policy Policy1 run started in background, please check 'fs _
-->policy status' for progress.
```

Resume the currently paused policy Policy1.
Create the schedule for the file system **lfs1**. The schedule runs every 10 minutes.

```
Storage> fs policy schedule create lfs1 */10 * * * *
ACCESS policy_schedule SUCCESS V-288-0 Schedule create for file system lfs1 done
        successfully.
```

Modify the schedule of the file system **lfs1**. The schedule runs every 20 minutes.

```
Storage> fs policy schedule modify lfs1 */20 * * * *
ACCESS policy_schedule SUCCESS V-288-0 Schedule modify for file system lfs1 done
        successfully.
```

List the schedule of the file system **lfs1**.

```
Storage> fs policy schedule list lfs1
File System Name  Minute Hour Day of Month Month Day of Week
----------------- ------ ----- --------------- ----- ---------------
lfs1              20    *    *              *    *
```

Remove the schedule of the file system **lfs1**.

```
Storage> fs policy schedule remove lfs1
ACCESS policy_schedule SUCCESS V-288-0 Schedule for file system lfs1 removed
        successfully.
```

Set the retention on the file **/vx/myfs/file1** 5y.

```
Storage> storage fs retention set /vx/myfs/file1 5y
ACCESS Retention SUCCESS V-288-0 Successfully set retention on /vx/myfs/file1
```

Set the retention on the file **/vx/myfs/file1** 05-20-2020.

```
Storage> storage fs retention set /vx/myfs/file1 05-20-2020
ACCESS Retention SUCCESS V-288-0 Successfully set retention on /vx/myfs/file1
```

Set the retention on the directory **/vx/myfs/dir1** 2y.

```
Storage> storage fs retention set /vx/myfs/dir1 2y
ACCESS Retention SUCCESS V-288-0 Applying retention on all current files in directory,
     this will take some time. Check report showevent for status.
```

Set the retention on the directory **/vx/myfs/dir1** 05-20-2020.

```
Storage> storage fs retention set /vx/myfs/dir1 05-20-2020
ACCESS Retention SUCCESS V-288-0 Applying retention on all current files in directory,
     this will take some time. Check report showevent for status.
```

Show the retention on the file **/vx/myfs/file1**

```
Storage> storage fs retention show /vx/myfs/file1
ACCESS Retention SUCCESS V-288-0 Retention value on file /vx/myfs/file1 is 06-08-2022
        23:12:51
```
Show the retention on the directory /vx/myfs/dir1

```
Storage> storage fs retention show /vx/myfs/dir1
ACCESS Retention ERROR V-288-0 Specified path is directory path, please give file path
```

Clear the retention on the file /vx/myfs/file1

```
Storage> storage fs retention clear /vx/myfs/file1
ACCESS Retention SUCCESS V-288-0 Successfully cleared retention on /vx/myfs/file1
```

Clear the retention on the directory /vx/myfs/dir1

```
Storage> storage fs retention clear /vx/myfs/dir1
ACCESS Retention SUCCESS V-288-0 Clearing retention of all current file in directory, this will take some time. Check report showevent for status.
```

Enable worm support for specified file system.

```
Storage> fs worm set fs1
ACCESS fs SUCCESS V-288-0 Enabled WORM for fs1 file system.
```

Disable worm support for specified file system.

```
Storage> fs worm clear fs1
ACCESS fs SUCCESS V-288-0 Disabled WORM for fs1 file system.
```

**16.1.5 SEE ALSO**

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1) compress(1) maxiops(1)
16.2 cloud

16.2.1 SYNOPSIS

cloud addservice service_name [service_provider=<service_provider>]
cloud listservice [service_name]
cloud removeservice service_name

16.2.2 DESCRIPTION

The storage cloud commands manage cloud storage configuration operations. The commands can be used to add, list, and remove user cloud storage subscriptions to Veritas Access.

16.2.3 OPTIONS

  service_provider=<service_provider> Specifies the cloud storage provider type. You can use Amazon Web Services (AWS) S3 or Glacier, or any S3-compatible cloud storage as the cloud service provider. If you are using an S3-compatible cloud provider, you need to specify the access key, secret key, and the REST endpoint to the fIservice_providerfp. The REST endpoint is the URL where your S3 server accepts the incoming requests. If an S3-compatible service cannot support AWS signature version 4, then it can not be added as a cloud service.

  cloud addservice service_name [service_provider=<service_provider>] Adds a public cloud subscription to Veritas Access as a cloud service with a name. The added subscription is accessed using service_name thereafter. You are prompted to provide the subscription credentials. To successfully send requests using AWS, you need to have a valid set of security credentials called access keys. You need to provide the access key and secret key as inputs. Credentials are verified and the service is added.

  cloud listservice [service_name] List added cloud services. If service_name is provided, then only that service is listed. Otherwise all configured services are listed.

  cloud removeservice service_name Remove the service service_name. Warning: Service removal fails if there are active cloud tiers associated with this service at the time of removal.

16.2.4 EXAMPLES

Add a new AWS service with name amzservice:

```
Storage> cloud addservice amzservice service_provider=AWS
Access_Key: ZTVhY2E3M2JlYWQyNWFk
Secret_Key: 
```

Add an S3-compatible cloud service provider with name isaobj:

```
Storage> cloud addservice isaobj service_provider=S3_COMPATIBLE
REST Endpoint: s3.isaobj:8143
Access_Key: ZTVhY2E3M2JlYWQyNWFk
Secret_Key: 
Successfully added new cloud service.
```
List all the configured cloud services.

<table>
<thead>
<tr>
<th>Storage&gt; cloud listservice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Provider</td>
</tr>
<tr>
<td>-------------------</td>
</tr>
<tr>
<td>amzservice AWS</td>
</tr>
<tr>
<td>isaobj S3_COMPATIBLE</td>
</tr>
</tbody>
</table>

Remove an existing cloud service named *amzservice*:

Storage> cloud removeservice amzservice

Remove an existing cloud service named *isaobj*:

Storage> cloud removeservice isaobj

16.2.5 SEE ALSO

tier(1), fs(1), disk(1)
16.3 compress

16.3.1 SYNOPSIS

compress file fs_name [file|dir] res_level [alg_strength] [file_pattern]
compress list fs_name [file|dir]
compress modage create fs_name file age_rule
compress modage remove fs_name
compress pattern create fs_name pattern_rule
compress pattern remove fs_name
compress schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]
compress schedule list fs_name
compress schedule remove sched_name
compress schedule show [sched_name]
compress schedule start fs_name sched_name res_level [alg_strength]
compress schedule stop fs_name
uncompress file fs_name file [file|dir] res_level

16.3.2 DESCRIPTION

The compress command performs administration functions for the Veritas Access compression feature. The compressed files keep the original name and do not change size, as reported by the stat or ls -l. However, the number of blocks allocated to the file as reported by the stat command or the ls -s command may be significantly reduced, depending on the compressibility of the data. The applications can access the files when compress is running, but it is recommended that compression jobs are scheduled during non-peak hours. The compression can be done using [low | medium | high] resource levels. The higher the resource level, the faster the job completes. Compression supports alg_strength 1 to 9 values. The default alg_strength is 6. Higher alg_strength increases storage savings, but it takes more time to complete.

16.3.3 OPTIONS

compress file fs_name file [file|dir] res_level [alg_strength] [file_pattern] Compress the file or directory of the fs_name file system using the specified res_level and alg_strength. The default alg_strength is 6. If the directory is specified, then all the files under the named directory are compressed. For directories, you can specify file name patterns. The res_level can be low, medium, or high.

compress list fs_name [file|dir] Lists the compression details for the fs_name file system files or directory.

compress modage create fs_name file age_rule Adds an age-based rule for scheduled compression jobs for the fs_name file system. The age_rule is specified in days.

compress modage remove fs_name Removes the age-based rule for the fs_name file system.

compress pattern create fs_name pattern_rule Adds a pattern-based rule for scheduled compression jobs for the fs_name file system.

compress pattern remove fs_name Removes the pattern-based rule for the fs_name file system.
**compress schedule create** sched_name duration minute [hour] [day] [month] [day_of_week] [node]
Create a compression sched_name schedule. The time and frequency of this schedule are specified using the command line in crontab format. This scheduled job runs on the specified [node]. If this node is not online at the time of the job, then this particular compression job runs on the CFS primary.

**compress schedule list fs_name** List the scheduled compression job details for the fs_name file system.

**compress schedule remove sched_name** Remove the compression sched_name schedule. Make sure none of the file systems have this sched_name assigned.

**compress schedule show [sched_name]** Show the compression sched_name schedule information. If sched_name is not specified, all the information about all the schedules are displayed.

**compress schedule start fs_name sched_name res_level [alg_strength]** Assign or start the compression sched_name schedule for the fs_name file system. The compression job uses resource and algorithm strength specified in arguments.

**compress schedule stop fs_name** Stop the scheduled compression schedule for the fs_name file system.

**uncompress file fs_name fl{file|dir} res_level** Uncompress the fs_name file system file or directory using the specified res_level.

### 16.3.4 EXAMPLES

Compress file data1.dbf in file system tpcc_arch1 using algorithm strength of 8 and high resource level.

Storage> compress file tpcc_arch1 data1.dbf high 8

Compress all files with pattern *.*.arch in directory test_dir on the tpcc_arch1 file system using the low resource level and algorithm strength of 3.

Storage> compress file tpcc_arch1 test_dir low 3 *.*.arch

List and display compression information for the files under the test_dir directory.

<table>
<thead>
<tr>
<th>%Comp</th>
<th>Physical</th>
<th>Logical</th>
<th>%Exts</th>
<th>Alg-Str</th>
<th>BSize</th>
<th>Filename</th>
</tr>
</thead>
<tbody>
<tr>
<td>92%</td>
<td>15.63 MB</td>
<td>200.0 MB</td>
<td>100%</td>
<td>gzip-3</td>
<td>1024k</td>
<td>test_dir/tpcc3.arch</td>
</tr>
<tr>
<td>87%</td>
<td>25.79 MB</td>
<td>200.0 MB</td>
<td>100%</td>
<td>gzip-3</td>
<td>1024k</td>
<td>test_dir/tpcc2.arch</td>
</tr>
<tr>
<td>89%</td>
<td>21.5 MB</td>
<td>200.0 MB</td>
<td>100%</td>
<td>gzip-3</td>
<td>1024k</td>
<td>test_dir/tpcc1.arch</td>
</tr>
<tr>
<td>0%</td>
<td>200.0 MB</td>
<td>200.0 MB</td>
<td>0%</td>
<td>-</td>
<td>-</td>
<td>test_dir/redo3.log</td>
</tr>
<tr>
<td>0%</td>
<td>200.0 MB</td>
<td>200.0 MB</td>
<td>0%</td>
<td>-</td>
<td>-</td>
<td>test_dir/redo2.log</td>
</tr>
<tr>
<td>0%</td>
<td>200.0 MB</td>
<td>200.0 MB</td>
<td>0%</td>
<td>-</td>
<td>-</td>
<td>test_dir/redo1.log</td>
</tr>
</tbody>
</table>

Uncompress all the files in test_dir directory with the medium resource level.

Storage> uncompress file tpcc_arch1 test_dir medium

Create a comp_sched_1 schedule that runs the compression job at 1:00 am every Saturday. This compression job should run only for 3 hours.

Storage> compress schedule create comp_sched_1 3 0 1 * * 6

Show the compression schedule details of the comp_sched_1 schedule.
Start compression schedule for the tpcc_arch1 file system with medium resource level and algorithm strength of 4. Compress files that are not modified in the last 5 days. Compress files with the name pattern *.arch only.

List the scheduled compression job status for the tpcc_arch1 file system.

16.3.5 SEE ALSO
disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), cifs(1)
16.4 fencing

16.4.1 SYNOPSIS

fencing destroy
fencing on disk [disk1, disk2, disk3]
fencing on majority
fencing off
fencing replace src_disk fIdest_disk
fencing status

16.4.2 DESCRIPTION

The storage fencing commands perform I/O fencing-related operations. These commands are not available in a single node set up.

16.4.3 OPTIONS

fencing destroy  Destroy coordinator pool. This command has no effect for majority-based fencing.

fencing on disk [disk1, disk2, disk3]  Enable disk-based I/O fencing on the three disks.

fencing on majority  Enable majority-based I/O fencing.

fencing off  Disable I/O fencing on all the nodes.

fencing replace src_disk dest_disk  Replace an existing coordinator disk with another disk. If the disk being replaced is in a failed state, then it is mandatory to delete the disk from the array. This is required because if the failed disk comes up and works properly, it can lead to an even number of I/O fencing disks, and this affects the functionality. This command has no effect for majority-based fencing.

fencing status  Check the I/O fencing status.

16.4.4 EXAMPLES

Destroy coordinator pool.

Storage> fencing destroy

Enable disk-based I/O fencing on the disks ams_wms0_000d, ams_wms0_000e, ams_wms0_000f (only three disks required).

Storage> fencing on disk ams_wms0_000d, ams_wms0_000e, ams_wms0_000f
ACCESS fencing Success V-288-0 IO Fencing feature now Enabled with SCSI3 Persistent Reservations
100% [#] Enabling fencing

Check I/O fencing status after enabling I/O fencing.
Storage> fencing status

IO Fencing Status
=================
Enabled

<table>
<thead>
<tr>
<th>Disk Name</th>
<th>Coord Flag</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams_wms0_000d</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ams_wms0_000e</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ams_wms0_000f</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Disable I/O fencing on all the nodes.

Storage> fencing off
ACCESS fencing Success V-288-0 IO Fencing feature now Disabled
100% [#] Disabling fencing

Check I/O fencing status after disabling I/O fencing.

Storage> fencing status

IO Fencing Status
=================
Disabled

<table>
<thead>
<tr>
<th>Disk Name</th>
<th>Coord Flag</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams_wms0_000d</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ams_wms0_000e</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>ams_wms0_000f</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Replace ams_wms0_000f with ams_wms0_000c with fencing in Enabled mode.

Storage> fencing replace ams_wms0_000f ams_wms0_000c
ACCESS fencing Success V-288-0 Replaced disk ams_wms0_000f with ams_wms0_000c successfully.
100% [#] Replacing disk ams_wms0_000f with ams_wms0_000c

Replace ams_wms0_000f with ams_wms0_000c with fencing in Disabled mode.

Storage> fencing replace ams_wms0_000f ams_wms0_000c
ACCESS fencing Success V-288-0 Replaced disk ams_wms0_000f with ams_wms0_000c successfully. Please run fencing on.
100% [#] Replacing disk ams_wms0_000f with ams_wms0_000c

Check I/O fencing status after I/O fencing replace operation completed.

Storage> fencing status

IO Fencing Status
=================
Disabled

<table>
<thead>
<tr>
<th>Disk Name</th>
<th>Coord Flag</th>
<th>On</th>
</tr>
</thead>
<tbody>
<tr>
<td>ams_wms0_000c</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>
Enable majority-based I/O fencing (no disks required).

```
Storage> fencing on majority
ACCESS fencing WARNING V-288-0 The IO may be interrupted while switching fencing state. Would you like to continue(yes/no):
yes
ACCESS fencing Success V-288-0 Majority Fencing Enabled
100% [#] Enabling fencing
```

Check I/O fencing status after enabling I/O fencing.

```
Storage> fencing status
IO Fencing Status
===============
Majority Fencing Enabled
```

Disable majority-based I/O fencing.

```
Storage> fencing off
ACCESS fencing WARNING V-288-0 The IO may be interrupted while switching fencing state. Would you like to continue(yes/no):
yes
ACCESS fencing Success V-288-0 IO Fencing feature now Disabled
100% [#] Disabling fencing
```

Check fencing status after disabling fencing.

```
Storage> fencing status
IO Fencing Status
===============
Disabled
```

16.4.5 SEE ALSO

disk(1), hba(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1)
16.5 dedup

16.5.1 SYNOPSIS

dedup enable fs_name [blksize]
dedup disable fs_name
dedup list [fs_name]
dedup start fs_name [node_name]
dedup stop fs_name
dedup status [fs_name]
dedup set cpu cpuvalue [fs_name]
dedup set memory memvalue
dedup set priority priorityval [fs_name]
dedup schedule set fs_name hours day [freq]
dedup schedule modify fs_name hours day [freq]
dedup schedule delete fs_name
dedup dryrun fs_name [threshold]
dedup remove fs_name

16.5.2 DESCRIPTION

The dedup command performs administration functions for the Veritas Access deduplication feature. The dedup command exposes interfaces for configuring deduplication and performing different deduplication actions. This includes operations such as enabling, disabling, starting, stopping, and removing deduplication on a file system. The dedup command also enables you to reset several deduplication configuration parameters and display the current deduplication status. Some configuration parameters can be set as local (specific to the file system) and/or global (applicable to all deduplication-enabled file systems). The local parameter overrides the value of the global parameter.

16.5.3 OPTIONS

**dedup enable fs_name [blksize]** Enable deduplication on a file system. Deduplication must be enabled for a file system before setting its configuration parameters and schedule. This command will also re-enable a deduplication schedule for a file system. The *blksize* option should be specified in bytes, for example, 4096. It should be a power of 2, multiple of file system’s block size and equal to or less than 128 K. Default block size is 0, which means that if the file system’s block size is less than 4096 bytes, then the dedup block size is set to 4096 bytes. Otherwise the dedup block size is set to the same as the file system’s block size.

**dedup disable fs_name** Disable deduplication schedule on a file system. Other information such as configuration, schedule, and the deduplication database remains intact.

*Warning:* Keeping deduplication disabled for longer periods of time may reduce the effectiveness of deduplication when it is re-enabled.
**dedup list [fs_name]** List the deduplication-configured file systems along with its granularity, state, schedule, and node list where it will run. Currently, node list is picked up automatically by the system and cannot be set by the user.

**dedup start fs_name [node_name]** Start deduplication manually. fs_name must be enabled for deduplication to start. You can specify the node for running the deduplication process.

**dedup stop fs_name** Stop the deduplication process running on a file system.

**dedup status fs_name** Display the current status of deduplication. It shows the file system name, saving’s amount, status, node where deduplication is either running or has completed, deduplication type i.e., SCHEDULED or MANUAL and other details.

**dedup set cpu cpuvalue [fs_name]** Set the CPU limit. This parameter can be set as global and/or local. Possible cpuval are idle and yield.

**dedup set memory memvalue** Set the memory limit in MB. It should be in a range of 128-4096 MB, default value is 128 MB. This can be set only as a global parameter.

**dedup set priority priorityval [fs_name]** Set the priority for deduplication-enabled file system(s). This parameter can be set as global and/or a local. Possible priorityval are low, normal, and high.

**dedup schedule set fs_name hours day [freq]** Set the schedule for the deduplication-enabled file system. This can be set only as a local parameter. Two categories of schedule are allowed i.e., run periodicity and type periodicity. The granularity of the schedule is limited to time of day and day of month. The hours can be specified as * (every hour), */N (every N hours) where N is in a range [1-12] or 5 comma-separated hours list in the range [0-23]. The day can be specified as * (every day), */N (every N days) where N is in the range [1-15] or any number in the range [1-7], where 1 means Sunday, 2 means Monday, and so on. The freq can be specified in the range 1-5. Default value is 1. A value of 4 means every 4th run deduplicates the file system, whereas the other runs consolidate the changes.

**dedup schedule modify fs_name hours day [freq]** Modify the deduplication schedule. The hours, day, and freq values can be specified. See the dedup schedule set command for the values.

**dedup schedule delete fs_name** Delete the deduplication schedule.

**dedup dryrun fs_name [threshold]** Initiate a deduplication dry run on the file system fs_name. This reports the approximate space saving. Dry run can be converted to the actual deduplication if it meets the threshold value.

**dedup remove fs_name** Remove deduplication configuration related information from the specified file system fs_name. This command removes all the configurations and the database specific to that file system.

*Warning:* This operation cannot be undone and re-running deduplication may take significant time.

### 16.5.4 EXAMPLES

Enable deduplication on the file system fs1:

```
Storage> dedup enable fs1 blksize=8192
```

Set the deduplication schedule:

```
Storage> dedup schedule set fs1 0,6,12,18 2 3
```
List the deduplication-enabled file system(s):

```
Storage> dedup list
Default Priority CPU Memory
--------------------------------------
NORMAL IDLE 128M
Filesystem Priority CPU Granularity Enabled Schedule NodeList
--------------------------------------------------------------------------------------
  /vx/fs1 NORMAL IDLE 8192B YES SET node_01,node_02
Show the deduplication parameters details on file system fs1:

Storage> dedup list fs1
Priority NORMAL
CPU IDLE
Memory 128M
Granularity 8192B
Enabled YES
Schedule hours Every hour
Schedule day interval Every Sunday
Schedule frequency 1
NodeList node_01,node_02
Check whether the dedup dry run reaches the threshold value of 60%:

Storage> dedup dryrun fs1 60
Show the deduplication status:

Storage> dedup status
Filesystem Saving Status Node Type Details
--------------------------------------------------------------------------------------
  /vx/fs1 00% COMPLETED node_01 MANUAL
  2011/05/23 17:08:00 Dryrun threshold not met. Cleaning up...
Start deduplication on all the file systems fs1:

Storage> dedup start fs1
Start deduplication on the file systems fs1 on node node_01:

Storage> dedup start fs1 node_01
Show the deduplication status:

Storage> dedup status
Filesystem Saving Status Node Type Details
--------------------------------------------------------------------------------------
  /vx/fs1 -- RUNNING node_01 MANUAL --
Show the status output after completion of deduplication:
### Storage> dedup status

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Saving</th>
<th>Status</th>
<th>Node</th>
<th>Type</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vx/fs1</td>
<td>34%</td>
<td>COMPLETED</td>
<td>node_01</td>
<td>MANUAL</td>
<td>2011/05/23 17:20:53 End detecting duplicates and file system changes 0</td>
</tr>
</tbody>
</table>

Remove deduplication on the file system *fs1*:

Storage> dedup remove fs1

List deduplication-enabled file systems:

<table>
<thead>
<tr>
<th>Filesystem</th>
<th>Priority</th>
<th>CPU</th>
<th>Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>/vx/fs1</td>
<td>NORMAL</td>
<td>IDLE</td>
<td>128M</td>
</tr>
</tbody>
</table>

### 16.5.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), cifs(1)
16.6 disk

16.6.1 SYNOPSIS

disk list [ stats | detail | paths ]

disk configure local <nodename> <vendor_id> <product_id> [serial_num]

disk grow disk_name

disk format disk1 [, disk2,...] [force]

disk remove disk1 [, disk2,...]

The disks may be direct-attached storage or shared storage devices. The format command enables network sharing of local disks, cluster wide. Also to grow a selected disk, if it is resized on the storage array. With format command, you can format the disk to “simple” format, if the disk does not belong to any disk groups.

16.6.2 DESCRIPTION

The disk list command displays aggregated information of all the disk devices connected to any or all of the nodes in the cluster.

The disk list stats command displays a list of disks and nodes in a tabular form. Each row corresponds to a disk, and each column corresponds to a node. An “OK” in the table indicates that the disk that corresponds to that row is accessible by the node that corresponds to that column. An “ERR” indicates that the disk that corresponds to that row is inaccessible by the node that corresponds to that column. A “NOT_CONN” indicates that the disk that corresponds to that row is not connected to the node that corresponds to that column.

The disk list detail command displays a list of disks and their properties. The column ID in disk list detail consists of: VendorID, ProductID, TargetID, and LunID. A “:” separates these fields.

If a disk is shared across multiple nodes and has name inconsistencies across the nodes, then that disk is shown as “—”. If a disk is shared across multiple nodes and has name inconsistencies across the nodes, then that disk is shown as “—”.

The disk list paths command shows the list of multiple paths of disks connected to all or any of the nodes in the cluster. It also shows the status of those paths on each node in the cluster.

The disk configure local <nodename> <vendor_id> <product_id> [serial_num] command adds local disks having the specified vendor ID and product ID in the JBOD category. The command can be used only on local disks which have locally-unique disk UDIDs. Else, UDID conflicts with other node’s local disks may occur. If you want to run this command on all the nodes, provide <nodename> argument as “all”. The <vendor_id> and <product_id> can be derived from the UDID of a disk. UDID is composed of <vendor_id>, <product_id>, cabinet serial number, and LUN serial numbers joined by underscore(or %5F). If the <vendor_id> or <product_id> has a space (or %20) in it’s name, replace it with ‘#’ and provide as one-word argument in the command. It may happen that the default location to get the serial number is invalid and hence the serial number in UDID will be filled with “0000”. This would still not make the UDID unique globally. serial_num should be given in the format opcode/pagecode/offset/length calculated carefully from the serial number format of the disk.

The disk grow disk_name increases the size of the specified disk. Before performing this operation, make sure that you increase the storage capacity of the disk on the storage array. Caution: When increasing the storage capacity of a disk, make sure that the storage array does not reformat it. This will destroy the data. For help, contact your Storage Administrator.

The disk format disk1 [,disk2,...] [force] command formats the disk. If the disk does not belong to any disk group, the format erases the first 100M space on the disk, and the disk is formatted using the vxdisksetup command. Use the force option to force formatting of disks with invalid configurations.
The `disk remove disk1 [,disk2...]` command removes the disks from the cluster configuration. This command is helpful in cases when the disk attributes are incorrectly listed in the system. Only the disks that are not a part of the pools can be removed. The command does not destroy the data on the disk, but just removes the disk from the system configuration. Rebooting the system or running `scanbus` brings back the disk to the system’s configuration. To remove the disk permanently from the system’s configuration, the Storage Administrator should remove the disk’s mapping from the array.

### 16.6.3 EXAMPLES

Display the list of disks in tabular form.

<table>
<thead>
<tr>
<th>Storage&gt; disk list stats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
</tr>
<tr>
<td>===</td>
</tr>
<tr>
<td>AMS_WM50_0</td>
</tr>
<tr>
<td>AMS_WM50_1</td>
</tr>
<tr>
<td>DS4800-0_0</td>
</tr>
<tr>
<td>DS4800-0_1</td>
</tr>
<tr>
<td>nasgw9_1_Disk_0</td>
</tr>
<tr>
<td>nasgw9_1_Disk_1</td>
</tr>
<tr>
<td>EMC_CLARiiON0_0</td>
</tr>
<tr>
<td>EMC_CLARiiON0_1</td>
</tr>
</tbody>
</table>

Display the list of disks and their properties.

<table>
<thead>
<tr>
<th>Storage&gt; disk list detail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
</tr>
<tr>
<td>===</td>
</tr>
<tr>
<td>ams_wms0_10</td>
</tr>
<tr>
<td>ams_wms0_11</td>
</tr>
<tr>
<td>ams_wms0_12</td>
</tr>
<tr>
<td>ams_wms0_13</td>
</tr>
<tr>
<td>ams_wms0_14</td>
</tr>
</tbody>
</table>

Show the list of multiple paths of disks connected to all or any of the nodes in the cluster. Also show the status of those paths on each node in the cluster.

<table>
<thead>
<tr>
<th>Storage&gt; disk list paths</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
</tr>
<tr>
<td>===</td>
</tr>
<tr>
<td>AMS_WM50_0</td>
</tr>
<tr>
<td>AMS_WM50_1</td>
</tr>
<tr>
<td>Disk_0</td>
</tr>
<tr>
<td>nasgw78_2_Disk_0</td>
</tr>
<tr>
<td>nasgw78_1_Disk_0</td>
</tr>
</tbody>
</table>

Add local disks having the specified vendor ID and product ID in the JBOD category. Before executing the command, note the ID.
Storage> disk list detail
Disk Pool Enclosure Array Type Size (Use%) Transport ID
vassd_01_disk_0 - disk 558.4G 0.0% SCSI DELL%5FPERC

Storage> disk configure local vassd_01 DELL PERC#H710 18/131/6/16
Please make sure that all disks from the given array are not in use. Continue? (y/n, default:n): y
ACCESS Disk SUCCESS V-288-0 Configured local disks on the node vassd_01 successfully.

After the command is executed, the ID changes. Disk name may also change as a consequence.

Storage> disk list detail
Disk Pool Enclosure Array Type Size (Use%) Transport ID
vassd_01_disk_2 - disk 558.4G 0.0% SCSI DELL%5FPERC

Storage> disk configure local all DELL PERC#H710
Please make sure that all disks from the given array are not in use. Continue? (y/n, default:n): y
ACCESS Disk SUCCESS V-288-0 Configured local disks on all the nodes successfully.

Grow a selected disk.

Storage> disk grow Disk_0
ACCESS disk SUCCESS V-288-0 disk grow Disk_0 completed successfully.

Format a specified disk.

Storage> disk format aluadisk0_6
You may lose all the data on the disk, do you want to continue (y/n, the default is _—n):y
disk format: aluadisk0_6 has been formatted successfully.

Storage> disk format aluadisk0_7, aluadisk0_8
You may lose all the data on the disk, do you want to continue (y/n, the default is _—n):y
ACCESS Disk SUCCESS V-288-0 disk format: aluadisk0_7 has been formatted successfully.

ACCESS Disk ERROR V-288-0 Disk aluadisk0_8 has invalid pool configuration. Format with force option to clean up else run scanbus to retrieve.
Storage> disk format aluadisk0_8 force
You may lose all the data on the disk, do you want to continue (y/n, the default is _—n):y
ACCESS Disk SUCCESS V-288-0 disk format: aluadisk0_8 has been formatted successfully.

Storage> disk format aluadisk0_7

310 Chapter 16. Storage Commands
You may lose all the data on the disk, do you want to continue (y/n, the default is n): y

ACCESS disk ERROR V-288-832 Disk aluadisk0_7 is used by pool pool_1, remove the disk from the use by command pool rmdisk firstly and then format.
ACCESS disk INFO V-288-832 File System fs_1 is based on the disk aluadisk0_7.
ACCESS disk INFO V-288-832 File System fs_2 is based on the disk aluadisk0_7.
ACCESS disk INFO V-288-832 File System fs_4 is based on the disk aluadisk0_7.

Remove a specified disk from configuration.

Storage> disk remove emc0_03ff
Removed disk emc0_03ff from nasgw78_1
Removed disk emc0_03ff from nasgw78_2

16.6.4 SEE ALSO

hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1)
16.7 fs

16.7.1 SYNOPSIS

fs create simple fs_name size pool1 [, disk1,...] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]

fs create mirrored fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]

fs create striped fs_name size ncolumns pool1 [, disk1,...] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]

fs create mirrored-stripe fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]

fs create striped-mirror fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]

fs create largefs simple fs_name size pool1 [blksize=<bytes>]
fs create largefs mirrored fs_name size nmirrors pool1 [blksize=<bytes>]
fs create largefs striped fs_name size ncolumns pool1 [stripeunit=<kilobytes> [blksize=<bytes>]

fs create largefs mirrored-stripe fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes> [blksize=<bytes>]

fs create largefs striped-mirror fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes> [blksize=<bytes>]

fs create pretuned fs_name size pool1 workload={virtualmachine|mediaserver} [layout={striped|striped-mirror|mirrored-stripe}] [ncolumns] [encrypt={on|off}]

fs defrag now fs_name time

fs destroy fs_name

fs list [fs_name]

fs online fs_name

fs offline fs_name
fs growto primary|secondary fs_name new_length [pool1 [, disk1,...] [protection=disk|pool]]
fs growby primary|secondary fs_name length_change [pool1 [, disk1,...]] [protection=disk|pool]
fs shrinkto primary|secondary fs_name new_length
fs shrinkby primary|secondary fs_name length_change
fs addmirror fs_name pool1 [, disk1,...] [protection=disk|pool]
fs rmmirror fs_name [pool_or_disk_name]
fs addcolumn fs_name ncolumns pool_or_disk_name
fs rmcolumn fs_name
tier addcolumn fs_name ncolumns pool_or_disk_name
tier rmcolumn fs_name
fs checkmirror
fs resync [fs_name]
fs checkresync
fs setfastresync fs_name [pool_or_disk_name]
fs unsetfastresync fs_name
fs fsck fs_name
fs alert set numinodes|numspace|fullspace value [fs_name,...] [snapshot_name]
fs alert unset numinodes|numspace|fullspace [fs_name,...] [snapshot_name]
fs alert show
fs upgrade fs_name
fs defrag schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]
fs defrag schedule remove sched_name
fs defrag schedule show [sched_name]
fs defrag schedule start fs_name sched_name
fs defrag schedule stop fs_name
fs defrag schedule list fs_name

fs policy add operation=move policy_name fs_name from_tier to_tier
   retrieval_option=Expedited|Standard|Bulk pattern [atime condition] [mtime condition]

fs policy add operation=delete policy_name fs_name from_tier
   pattern [atime condition] [mtime condition]

fs policy modify policy_name pattern [atime condition] [mtime condition]
fs policy delete policy_name fs_name
fs policy rename old_policy_name new_policy_name
fs policy list [fs_name]
fs policy run policy_name
fs policy dryrun policy_name
fs policy status policy_name
fs policy abort policy_name
fs policy pause policy_name
fs policy resume policy_name
fs policy schedule create fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
fs policy schedule modify fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
fs policy schedule remove fs_name
fs policy schedule list fs_name
fs retention set path rtime
fs retention show path
fs retention clear path
fs worm set fs_name
fs worm clear fs_name
""fs setmaxiops " [fs_name] maxiops
fs maxiopslist [fs_name]
fs iopsstat list [fs_name]
fs iopsstat reset [fs_name]

16.7.2 DESCRIPTION

The storage fs commands manage file system operations.

File systems consist of metadata and file data. Metadata consists of information like last modification time, creation time, permissions, and so on. The total amount of space taken by the metadata depends upon the number of files. A file system that contains many small files requires more space to store the metadata, and a file system with fewer large files requires less space for storing the metadata.

When a file system is created, some space is set aside initially for the metadata. This space is generally proportional to the size of the file system. This is the reason for the non-zero usage percentage in the output of fs list just after the creation of the file system. The space set aside for the metadata grows or shrinks as and when required. A file system on a 1 GB volume takes around 40 MB (about 4%) initially for storing the metadata, whereas a file system of size 10 MB takes around 7.3 MB (73%) initially for storing the metadata.

Veritas Access provides a scale-out file system that manages a single namespace spanning over both on-premises storage as well as cloud storage, which provides better fault tolerance for large data sets. Unlike a standard file system, a scale-out file system is Active/Passive, which means that the file system can be online on only one node of the cluster at a time. A scale-out file system is always active on the node where its virtual IP address is online. A virtual IP address is associated with a scale-out file system when the system is created. You can find what virtual IP address is associated with a scale-out file system by using the NFS> share show command.

Veritas Access supports access to a scale-out file systems using NFS-Ganesha and S3. NFS shares that are created for scale-out file systems must be mounted on the NFS clients using the virtual IP address that is associated with the scale-out file system, similarly S3 buckets created on scale-out file system must be accessed using the same virtual IP
address. You can find the virtual IP address associated with a scale-out file system by using the `NFS> share show` command or using `objectaccess> bucket show` command based on the protocol you are using.

S3 buckets created on scale-out file system must be accessed using a virtual-hosted-style URL (rather than the path-style URL) and S3 client’s DNS must be updated to this virtual IP address for the corresponding virtual-hosted-style URL. If a bucket `bucket1` is created by the S3 client, then its virtual-hosted-style URL would be `bucket1.s3.cluster_name:8143`, where `cluster_name` is the Veritas Access cluster name and 8143 is the port on which the Veritas Access S3 server is running.

A scale-out file system is structured as a layered file system that includes a set of storage containers. The data that is stored in the cloud can be one of the storage containers. One on-premises storage container stores the metadata and all the other containers (on-premises and cloud) store the actual data. This modular structure allows the scale-out file system to be more resilient in cases where high capacity or fault tolerance is needed. A scale-out file system accomplishes this without compromising on file system performance.

**Scale-out file system specifications**

- Twenty percent of a scale-out file system’s size is devoted to the metadata container.
- The maximum size of a metadata container is 10 TB.
- The minimum size of a scale-out file system is 10 GB.
- The maximum size of a scale-out file system is 3 PB.
- You can grow the scale-out file system up to 3 PB.
- To create or grow a scale-out file system above 522 TB, you need to provide the file system size in multiples of 128 GB.
- You can shrink the scale-out file system only if its size is less than 522 TB.

New storage containers are created when you grow the scale-out file system beyond 522 TB. The pool on which the scale-out fs is created will be used to create these new containers. There will also be a data movement to these new storage containers so that data is distributed evenly among all the storage containers.

The following types of clouds can be added as storage containers for scale-out fs, Amazon S3, Amazon Glacier, AWS GovCloud(US), Azure, Google cloud, Alibaba, Veritas Access S3 and any S3-compatible storage provider. The data is always written to the on-premises storage container and then data can be moved to the cloud container using a tiering mechanism. File metadata including any attributes set on the file resides on-premises eventhough file is moved to cloud. This cloud as a tier feature is best used for moving infrequently accessed data to the cloud.

Amazon Glacier is an offline cloud tier, which means that data moved to Amazon Glacier cannot be accessed immediately. An EIO error is returned if you try to read, write, or truncate the files moved to the Amazon Glacier tier. If you want to read or modify the data, move the data to on-premises using `tier move` or using policies. The data will be available after some time based on the Amazon Glacier retrieval option you selected.

When Amazon S3, AWS GovCloud(US), Azure, Google cloud, Alibaba, Veritas Access S3 and any S3-compatible storage providere is used as the cloud tier, the data present on these clouds can be accessed any time (Unlike in Amazon Glacier). An EIO error is returned if you try to write, or truncate the files moved to these clouds. If you want to modify the data, move the data to on-premises using `tier move` or using policies.

**Note:** You cannot use the CIFS protocol with a scale-out file system.

**Note:** Not all of the storage commands are supported for scale-out file systems.

### 16.7.3 OPTIONS

- `size` Size of the file system (for example 10m, 10M, 25g, 100G).
**nmirrors**  Number of mirrors.

**ncolumns**  Number of columns.

**protection=disk**  If the protection is set to `disk`, then mirrors are created on separate disks. This flag works only for the file systems of type mirrored, mirrored-striped, and striped-mirror. The disks may or may not be in the same pool.

**protection=pool**  If the protection is set to `pool`, then mirrors are created in separate pools. This flag works only for the file systems of type mirrored, mirrored-striped, and striped-mirror. If not enough space is available, then the file system creation operation fails. The `protection=pool` option is not supported for an isolated pool. If the file system is created with the `protection=pool` option, then both pools in question cannot be merged to create a single pool, which defeats the purpose of `protection=pool`.

**stripeunit=<kilobytes>**  Set the stripe width of the file system, where possible values of kilobytes are 128, 256, 512, 1024, and 2048.

**blksize=<bytes>**  Set the block size of the file system, where possible values of bytes are 1024, 2048, 4096, and 8192. Default block size is 8192.

**pdir_enable={yes|no}**  Enable or disable partition directory for the file system. The default value is `pdir_enable=no`, which means partition directory is disabled for the file system.

**encrypt={yes|no}**  Specify whether to create the file system on encrypted volume. If set to `on`, file system is created on encrypted volume. The default value is `encrypt=off`.

**worm={yes|no}**  Specify whether to create a worm-enabled file system. If set to `yes`, file system is created with WORM support enabled. The default value is `worm=no`.

**workload={virtualmachine|mediaserver}**  Type of workload using this file system. The workload type cannot be changed after the file system is created. If the workload type is virtualmachine, then all the files in the file system have a minimum extent size of 1MB. This reduces the file system fragmentation and improves virtual machine I/O performance.

**layout={striped|striped-mirror|mirrored-stripe}**  Layout of the underlying volume on which the file system is created. The default value is `layout=striped`.

### 16.7.4 COMMAND DESCRIPTIONS

**fs create simple**  `fs_name size pool1 [, disk1,...] [blksize=<bytes> [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]`  
Create a simple file system with the specified size on one of the specified pools/disks and make it online.

**fs create mirrored**  `fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]`  
Create a mirrored file system with the specified number of mirrors and make it online.

**fs create striped**  `fs_name size ncolumns pool1 [, disk1,...] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]`  
Create a striped file system with the specified number of stripes and make it online.

**fs create mirrored-stripe**  `fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]`  
Create a mirrored-striped file system with a specified number of mirrors and stripes and make it online.

**fs create striped-mirror**  `fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>] [blksize=<bytes>] [pdir_enable={yes|no}] [encrypt={on|off}] [worm={yes|no}]`  
Create a striped-mirror file system with the specified number of mirrors and stripes and make it online.
Create a striped-mirrored file system with a specified number of mirrors and stripes and make it online.

```
fs create largefs simple fs_name size pool1 [blksize=<bytes>]
```

Create a largefs file system with the specified size on pools/disks specified and bring it online.

```
fs create largefs mirrored fs_name size nmirrors pool1 [blksize=<bytes>]
```

Create a mirrored largefs file system with the specified number of mirrors and make it online.

```
fs create largefs striped fs_name size ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a striped largefs file system with the specified number of stripes and make it online.

```
fs create largefs mirrored-stripe fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a mirrored-striped largefs file system with a specified number of mirrors and stripes and make it online.

```
fs create largefs striped-mirror fs_name size nmirrors ncolumns pool1 [stripeunit=<kilobytes>] [blksize=<bytes>]
```

Create a striped-mirrored largefs file system with a specified number of mirrors and stripes and make it online.

```
fs create pretuned fs_name size pool1 workload={virtualmachine|mediaserver} [layout={striped|striped-mirror|mirrored-stripe}] [ncolumns] [encrypt={on|off}]
```

Create a file system with the specified size using the disks from the specified pool. The volume is created with the specified layout. Stripe the volume across the specified number of columns with 512 K as the stripe size. Tune the file system for the specified workload.

```
fs defrag now fs_name time
```

Defragment a file system now. The `time` value should be larger than 1 minute or infinite.

```
fs destroy fs_name
```

Destroy a file system.

```
fs list [fs_name]
```

List all the file systems.

```
fs online fs_name
```

Make the file system online.

```
fs offline fs_name
```

Make the file system offline.

```
fs growto primary|secondary fs_name new_length [pool1 [, disk1,...]] [protection=disk|pool]
```

Grow the file system’s primary or secondary tier to a specified size. If no pool is specified with the command, the disks for growing the file system can be taken from any available pool. The protection flag takes the default value of “disk” in this case. The value of protection field cannot be set to “pool” when no pool is specified with the command. This operation may convert the layout of the file system if the command determines that the new file system is too large for the original layout.

If the file system specified is a scale-out file system (largefs type), growing the primary tier grows the default disk tier. Growing the secondary tier is not supported for a scale-out file system.

```
fs growby primary|secondary fs_name length_change [pool1 [, disk1,...]] [protection=disk|pool]
```
Grow the file system’s primary or secondary tier by a specified size. If no pool is specified with the command, the disks for growing the file system can be taken from any available pool. The protection flag takes the default value of disk in this case. The value of protection field cannot be set to pool when no pool is specified with the command. This operation may convert the layout of the file system if the command determines that the new file system is too large for the original layout. See the description of fs growto for more information if you resize a scale-out file system.

```bash
fs shrinkto primary|secondary fs_name new_length
```

Shrink the file system’s primary or secondary tier to a specified size.

See the description of fs growto for more information if you resize a scale-out file system.

```bash
fs shrinkby primary|secondary fs_name length_change
```

Shrink the file system’s primary or secondary tier by a specified size.

See the description of fs growto for more information if you resize a scale-out file system.

```bash
fs addmirror fs_name pool1 [, disk1...] [protection=disk|pool]
```

Add a mirror to the file system.

```bash
fs rmmirror fs_name [pool_or_disk_name]
```

Remove a mirror from the file system that is spanning on the specified pools/disks. If a pool name is the same as a disk name, then the mirror present on the pool is deleted.

```bash
fs addcolumn fs_name ncolumns pool_or_disk_name
```

Add the specified number of columns to the file system. In case of a striped file system, the number of disks specified should be equal to ncolumns. In case of mirrored-stripe and striped-mirror, the disks specified should be equal to ( ncolumns * number_of_mirrors_in_fs ).

```bash
fs rmcolumn fs_name
```

Remove a column from the file system.

```bash
tier addcolumn fs_name ncolumns pool_or_disk_name
```

Add specified number of columns to the secondary tier of the file system. In case of a striped file system, the number of disks specified should be equal to ncolumns. In case of mirrored-stripe and striped-mirror, the disks specified should be equal to ( ncolumns * number_of_mirrors_in_fs ).

```bash
tier rmcolumn fs_name
```

Remove a column from the secondary tier of a file system.

```bash
fs checkmirror
```

Show file systems that have stale mirrors.

```bash
fs resync [fs_name]
```

Resynchronize all stale mirrors for all file systems or for a certain file system.

```bash
fs checkresync
```

Show resynchronization and rollback synchronization progress running in the background.

```bash
fs setfastresync fs_name [pool_or_disk_name]
```

Enable fast resync for the specified file system.

```bash
fs unsetfastresync fs_name
```

Disable fast resync for the specified file system.
fs fsck fs_name

Check and repair the specified file system.

Scale-out fsck checks the consistency of the metafs, the datafs, and the database and repairs any inconsistencies found. Scale-out fsck checks if the metafs and datafs are marked for fullfsck, and if yes, it performs a fullfsck (check and repair) of the corresponding file systems. Based on the actions taken by fsck on the individual file systems, Scale-out fsck repairs the inconsistencies in other parts of the scale-out file system. Scale-out fsck goes through all the file handles present in the database and checks if the corresponding metafs and datafs file handles are consistent with each other. For example, in some cases, fullfsck might delete files from the datafs. To maintain consistency, corresponding metafs files and other datafs files are removed, and the corresponding key is removed from the database.

fs alert set numinodes|numspace|fullspace value [fs_name] [snapshot_name]

Allow users to set alerts on file systems and snapshot usage. The user can set alerts based on the number of inodes used or the file system space used. The value should be in a percentage when the alert is being set for the disk space. The default alert set for the disk space usage is at 80%. When the alert set is numinodes, the input should be the number of inodes. The default alert value for numinodes is set at 0. This will not send any alert till you set it to a different value. When this command is not supplied with the file system name, it changes the default system wide value for the alerts. For the file systems on which alerts are set explicitly, the alert is sent based on the value specified and not the default value. The alerts can be observed by the user in the “Report> showevents” CLI command. You can specify a comma-separated list of file systems.

fullspace is the tunable for file system full protection. For the file system to run efficiently, users should always reserve some space for the file system, instead of using 100% of the space. When file system usage is above the limit set by fullspace, all the NFS/CIFS shares on top of the file system are automatically changed to readonly to prevent the file system from becoming full. When users grow the file system or delete some files to get enough free space, the shares are automatically changed back to readwrite (there might be a delay for up to 5 minutes). By default, fullspace is 0, which means this function is disabled.

fs alert unset numinodes|numspace|fullspace [fs_name] [snapshot_name]

Allow users to unset the alerts set on the file system and the snapshot name. If an alert on any file system is unset, the user gets an alert for the file system based on the default values. You can specify a comma-separated list of file systems. When fullspace is unset (or set to 0), the shares that were changed to readonly due to file system high usage are changed back to readwrite mode immediately.

fs alert show

Show the current disk space usage and the alert value set. “(D)” beside the value shows that the value is the default value through the system.

fs upgrade fs_name

This command upgrades the file system layout to version 13. The file system needs to be online for this command to proceed. The version information about the file system is displayed in the fs list fs_name command.

fs defrag schedule create sched_name duration minute [hour] [day] [month] [day_of_week] [node]

Create a defrag schedule. The time and frequency of this schedule are specified in the command line in crontab format. This scheduled job runs on the node specified. If this node is not online at the time of the job, then this particular defrag job runs on the CFS primary. The scheduled defrag job may last up to the specified duration hours or minutes.

fs defrag schedule remove sched_name

Remove the defrag schedule by name sched_name. Make sure none of the file systems have this sched_name assigned.
fs defrag schedule show [sched_name]
Show the defrag schedule information for the schedule by name sched_name. If sched_name is not specified, all the information about all the schedules are displayed.

fs defrag schedule start fs_name sched_name
Assign or start the defrag schedule by name sched_name for the file system by name fs_name.

fs defrag schedule stop fs_name
Stop the scheduled defrag schedule for the file system by name fs_name.

fs defrag schedule list fs_name
List the scheduled defrag job details for the file system by name fs_name.

fs policy add operation=move policy_name fs_name from_tier to_tier retrieval_option=Expedited|Standard|Bulk pattern [atime condition] [mtime condition]
Create a data movement policy for the scale-out file system fs_name. The policy moves files and directories that meet the criteria from the source tier (from_tier) to the destination tier (to_tier). Movement can be from the cloud tier to a disk tier or from a disk tier to the cloud tier.

The retrieval option determines the time needed to move files from Amazon Glacier to on-premises. This option is not used when moving files from on-premises to Amazon Glacier.

Expedited retrievals typically complete within 1-5 minutes. The expedited option is expensive and you should use it conservatively. Files moved from the Amazon Glacier tier with the expedited option might return with the following error: InsufficientCapacityException (503 service unavailable). This error occurs if there is insufficient capacity to process the expedited request. This error only applies to expedited retrievals and not to standard or bulk retrievals.

Standard retrievals typically complete within 3-5 hours.

Bulk retrievals typically complete within 5-12 hours. Bulk is the default option.

Note: The maximum file size for moving files to AWS Glacier is 4 GB.

Pattern identifies the files or directories that you want to move between tiers. Pattern is required. You can further restrict the files or directories to move by specifying the last accessed time (atime) or the last modified time (mtime). The atime and mtime criteria are optional.

fs policy add operation=delete policy_name fs_name from_tier pattern [atime condition] [mtime condition]
Create a data deletion policy for the scale-out file system fs_name. The policy deletes files and directories that meet the criteria from the specified tier (from_tier). Pattern identifies the files or directories that you want to delete. Pattern is required. You can further restrict the files or directories to delete by specifying the last accessed time (atime) or the last modified time (mtime). The atime and mtime criteria are optional.

fs policy modify policy_name pattern [atime condition] [mtime condition]
Modifies the pattern, atime, and mtime search criteria for the file movement or deletion of the policy. atime and mtime are optional criteria. You cannot change the policy operation, or change the storage tiers that were specified when the policy was created.

fs policy delete policy_name fs_name
Stop any data movement or data deletion policy that was set for a file system. You cannot delete a policy if the policy is running.

fs policy rename old_policy_name new_policy_name
Rename an existing policy to a new policy name. You cannot rename a policy if the policy is running.

```
fs policy list [fs_name]
```

List all the data movement and data deletion polices that are set for all the file systems. If `fs_name` is included in the command, then the command lists all the policies for the specified file system.

```
fs policy run policy_name
```

Move or prune files according to the configured file system policy `policy_name`. The policy runs in the background until it completes, or until you abort or pause the policy. File system policies are configured only for scale-out file systems (largefs type). The policy runs on the node on which the scale-out file system is active. If a policy run encounters an error, it is retried five times before the run is aborted. If the policy is already active but paused, you are prompted whether you want to resume the paused job or to start a new run. You cannot run a policy that is already running, because of a schedule or a previous `fs policy run` command. You also cannot run a policy if a tier move command is running for the same path or file system.

```
fs policy dryrun policy_name
```

Perform a dry run of the file system policy `policy_name`. This command previews the running of the policy but does not actually move or prune any files. Use this command to estimate the I/O activity involved if the policy is run. The dry run collects the statistics such as the number of files and the amount of data that will be moved. You cannot perform a dryrun if the policy is already running, or if a tier move command is running on the same path or file system.

```
fs policy status policy_name
```

Show the status of the currently running policy or dry run of the policy `policy_name`. If the policy is not currently running, the status shows the most recent run. The information includes the type of the run (normal or dry run), the status, the total data, the amount of data moved so far, the number of files, the number of files moved or deleted so far, and the name of the last file completed by the policy run.

```
fs policy abort policy_name
```

Aborts the currently executing policy run or dry run for the policy `policy_name`. The abort is immediate and interrupts any data movement in progress. The aborted policy cannot be resumed using the `fs policy resume` command. If you need to restart the policy, start a new run with the `fs policy run` command.

```
fs policy pause policy_name
```

Pause the currently executing policy run or dry run for the policy `policy_name`. The pause is immediate and interrupts any data movement in progress. You can resume the policy using the `fs policy resume` command. You can abort the paused policy using the `fs policy abort` command. When you pause a policy, the scheduled runs of the policy are also skipped until the policy is resumed.

```
fs policy resume policy_name
```

Restart the policy run or dry run that was paused with the `fs policy pause` command. The policy resumes from the point where the policy run was interrupted.

```
fs policy schedule create fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
```

Create the file system policy schedule for the file system `fs_name`. The schedule uses a time format similar to the format used in UNIX cron configuration files.

The schedule applies to the file system policies created using the `fs policy create` command. When a schedule is set for a particular file system, all the policies for that file system are started at the scheduled times. If any policy is paused using the `fs policy pause` command, the policy does not run at the scheduled time. The policy is skipped until the policy is resumed using the `fs policy resume` command.
About the schedule format:

A schedule is specified in a format similar to the UNIX crontab format. The format uses five fields to specify when the schedule runs:

- **minute**: Enter a numeric value between 0-59, or an asterisk (*), which represents every minute. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- **hour**: Enter a numeric value between 0-23, or an asterisk (*), which represents every hour. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- **day_of_the_month**: Enter a numeric value between 1-31, or an asterisk (*), which represents every day of the month. You can also enter a step value (*/x), or a range of numbers separated by a hyphen.

- **month**: Enter a numeric value between 1-12, or an asterisk (*), which represents every month. You can also use the names of the month. Enter the first three letters of the month (you must use lowercase letters). You can also enter a step value (*/x), or a range.

- **day_of_the_week**: Enter a numeric value between 0-6, where 0 represents Sunday, or an asterisk (*), which represents every day of the week. You can also enter the first three letters of the week (you must use lowercase letters). You can also enter a step value (*/x), or a range.

A step value (*/x) specifies that the schedule runs at an interval of x. The interval should be an even multiple of the field’s range. For example, you could specify */4 for the hour field to specify every four hours, since 24 is evenly divisible by 4. However, if you specify */15, you may get undesired results, since 24 is not evenly divisible by 15. The schedule runs after 15 hours, then 7 hours.

A range of numbers (two values separated by a hyphen) represents a time period during which you want the schedule to run.

Examples:

To run the schedule every two hours every day: 0 */2 * * *

To run the schedule on 2:00 a.m. every Monday: *2 * * 1

To run the schedule at 11:15 p.m. every Saturday: 15 23 * * 6

```
fs policy schedule modify fs_name [minute] [hour] [day_of_the_month] [month] [day_of_the_week]
```

Modify the file system policy schedule for the file system `fs_name`. The schedule uses a time format similar to the format used in UNIX cron configuration files. Refer to the `fs policy schedule create` section for the detailed description of the schedule format.

```
fs policy schedule remove fs_name
```

Remove the file system policy schedule associated with the file system `fs_name`.

```
fs policy schedule list fs_name
```

List the file system policy schedule associated with the file system `fs_name`.

```
fs retention set path rtime
```

Sets the retention on a file path `path` or on all the files that are currently present in specified path `path`. `rtime` can be in [1-9]d|D|m|M|y|Y) or mm-dd-yyyy format.

```
fs retention show path
```

Shows the retention value applied on the specified file path `path`.

```
fs retention clear path
```

Clears the retention on a file path `path` or on all the files that are currently present in specified path `path`.

```
fs worm set fs_name
```

Enable worm support for the specified file system.

```
fs worm clear fs_name
```

Disable worm support for the specified file system.

```
"fs setmaxiops " [fs_name] maxiops
```

Chapter 16. Storage Commands
set/reset MAXIOPS on a file system

```plaintext
fs maxiopslist

List the value of maximum I/O operations per second (MAXIOPS) set on all the file systems.
```

```plaintext
fs iopsstat list [fs_name]

Display a statistical view of the maximum I/O operations per second (MAXIOPS) for a file system.
```

```plaintext
fs iopsstat reset [fs_name]

Reset the MAXIOPS statisticis instead of printing them.
```

### 16.7.5 EXAMPLES

Create a mirrored file system with name `fs1` with disks from the pools `pool1` and `pool2`.

```
Storage> fs create mirrored fs1 100M 2 pool1,pool2
100% [#] Creating mirrored filesystem
```

Add a mirror to file system `fs1`.

```
Storage> fs addmirror fs1 pool3,pool4
```

Remove a mirror from file system `fs1` residing on Disk AMS_WMS0_0.

```
Storage> fs rmmirror fs1 AMS_WMS0_0
```

Add two columns to file system `fs1`.

```
Storage> fs addcolumn fs1 2 pool3
```

Remove column from file system `fs1`.

```
Storage> fs rmcolumn fs1
```

Add two columns to the secondary tier of file system `fs1`.

```
Storage> tier addcolumn fs1 2 pool3
```

Remove column from the secondary tier of file system `fs1`.

```
Storage> tier rmcolumn fs1
```

Show file systems that have stale mirrors.

```
Storage> fs checkmirror
fs_name:
--------
mirror3
```

Resynchronize all stale mirrors for all file systems.

```
Storage> fs resync
Resync stale mirrors for file systems that are started in the background.
```

Resynchronize all stale mirrors for a certain file system.

```
```
Storage> fs resync mirror3
Resync stale mirror for file system mirror3 is started in background.

Show resynchronization progress running in the background.

Storage> fs checkresync
FS MIRROR TYPE PROGRESS START_TIME
  -> USED_TIME REMAINING_TIME
============================================================================================================
mir2 tier 1,mirror 02 RESYNC 6.46% Jun/05/2011/09:39:53
('0:5:9 1:14:34
mir3_roll2 tier 1 ROLLBACK 1.28% Jun/05/2011/14:51:40
('0:0:12 15:23
mir3 tier 1,mirror 03 RESYNC 7.67% Jun/05/2011/15:10:26
('0:1:14 14:50

Make a file system offline.

Storage> fs offline fs1
100% [#] Offline filesystem

Check and repair a file system while it is in offline state. It tries normal fsck first, if fullfsck flag is set, it proceeds further accordingly based on the given input.

Storage> fs fsck fs1
Do you want to do fsck without log replay? yes|no
n
File system fs1 fsck successfully

Storage> fs fsck fs1
Do you want to do fsck without log replay? yes|no
y

File system fs1 fsck successfully

Storage> fs fsck fs1
Do you want to do fsck without log replay? yes|no
n
File system fs1 marked for full fsck.Running full fsck may take long time for completion.

Do you want to continue? yes|no
n
File system fs1 full fsck canceled.

Storage> fs fsck fs1
Do you want to do fsck without log replay? yes|no
n
File system fs1 marked for full fsck.Running full fsck may take long time for completion.

Do you want to continue? yes|no
y

Check the fullfsck status by running the command again.

Storage> fs list mir3
General Info:

324 Chapter 16. Storage Commands
<table>
<thead>
<tr>
<th>Block Size: 1024 Bytes</th>
<th>Version: Version 11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster5_01: online</td>
<td></td>
</tr>
</tbody>
</table>

**Primary Tier**

---

- **Size:** 30.00G
- **Use%:** 0%
- **Layout:** mirrored
- **Mirrors:** 4
- **Columns:** -
- **Stripe Unit:** 0.00 K
- **FastResync:** Enabled

1. Mirror 01:
   - List of pools: pool1
   - List of disks: disk1 disk2

2. Mirror 02:
   - List of pools: pool1
   - List of disks: disk3 disk4

3. Mirror 03:
   - List of pools: pool1
   - List of disks: disk5 disk6

4. Mirror 04:
   - List of pools: pool1
   - List of disks: disk7 disk8

**Secondary Tier**

---

- **Size:** 20.00G
- **Use%:** 0%
- **Layout:** mirrored
- **Mirrors:** 2
- **Columns:** -
- **Stripe Unit:** 0.00 K
- **FastResync:** Disabled

1. Mirror 01:
   - List of pools: pool1
   - List of disks: disk9 disk10

2. Mirror 02:
   - List of pools: pool1
   - List of disks: disk11 disk12

**FS Type:** Normal

**Defrag Status:** Not Running
**Fullfsck Status:** Not Running
**Resync Status:**

- Tier 1, Mirror 03: 7.67%
  - Start_time: Jun/05/2011/15:10:26
  - Work_time: 0:1:14
  - Remaining_time: 14:50

- Tier 1, Mirror 04: 1.08%
  - Start_time: Jun/05/2011/13:08:07
  - Work_time: 0:1:21
  - Remaining_time: 2:03:33

- Tier 2, Mirror 02: 11.27%
  - Start_time: Jun/05/2011/14:03:14
  - Work_time: 0:0:18
  - Remaining_time: 02:21
Rollsync Status:

Rollsync mir3_roll2, Tier 1: 1.28% Start_time: Jun/05/2011/14:51:40 Work_time: 0:0:12 Remaining_time: 15:23
Relayout Status: Not Running

Make a file system online.

Storage> fs online fs1
100% [&#35;] Online filesystem

Check and repair a file system while it is in offline state.

Storage> fs fsck fs1
ACCESS fs ERROR V-288-693 fs1 must be offline to perform fsck.

Grow file system’s primary tier size to 1 G.

Storage> fs growto primary fs1 1g

Grow file system’s primary tier size by 50 M.

Storage> fs growby primary fs1 50M

Shrink file system’s primary tier by specified size.

Storage> fs shrinkby primary fs1 10m

Shrink file system’s primary tier to just 50 M.

Storage> fs shrinkto primary fs1 50M

View the list of file systems.

Storage> fs list

<table>
<thead>
<tr>
<th>FS</th>
<th>STATUS</th>
<th>SIZE</th>
<th>LAYOUT</th>
<th>MIRRORS</th>
<th>COLUMNS</th>
<th>USE%</th>
<th>NFS</th>
<th>CIFS</th>
<th>FTP</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SECONDARY</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>===</td>
<td>=======</td>
<td>======</td>
<td>=======</td>
<td>=======</td>
<td>=======</td>
<td>=====</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs1</td>
<td>online</td>
<td>100.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>3%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs2</td>
<td>online</td>
<td>100.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>3%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs3</td>
<td>online</td>
<td>700.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>4%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs4</td>
<td>online</td>
<td>69.00M</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>4%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs5</td>
<td>online</td>
<td>1.94G</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>1%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>yes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fs6</td>
<td>online</td>
<td>1.94G</td>
<td>simple</td>
<td>-</td>
<td>-</td>
<td>1%</td>
<td>no</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>yes,metaOk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Display detailed information for a specific file system.

Storage> fs list fs6
General Info:
===============
Block Size: 1024 Bytes
Version: Version 11
node_01: online
defnode_02: offline
def
Primary Tier
===========
Size: 500.00M
Use%: 0%
Layout: mirrored
Mirrors: 2
Columns: -
Stripe Unit: 0.00 K
FastResync: Enabled

1. Mirror 01:
   List of pools: p03
   List of disks: ams_wms0_12

2. Mirror 02:
   List of pools: p03
   List of disks: ams_wms0_13

FS Type: Normal

Defrag Status: Not Running
Fullfsck Status: Not Running
Resync Status: Not Running
RollSync Status: Not Running
Relayout Status: Not Running

Disable FastResync for a file system.

Storage> fs unsetfastresync fs6

Try disabling FastResync for a file system where it is already in disabled state.

Storage> fs unsetfastresync fs6
ACCESS fs ERROR V-288-655 Fastresync is not enabled for fs6.

Enable FastResync for a file system.

Storage> fs setfastresync fs6

Try enabling FastResync for a file system where it is already in enabled state.

Storage> fs setfastresync fs6
ACCESS fs ERROR V-288-651 File system fs6 is already fastresync enabled.

Defragment a file system.

Storage>fs defrag fs0 1H10M
The file system fs0 is offline, please online fs0 before defragmentation

Storage>fs defrag fs1 1H10M
it will take some time to do the defragmentation
do you want to continue? yes|no
n
Defragmentation cancelled for fs1
Storage>fs defrag fs1 1H10M
it will take some time to do the defragmentation
do you want to continue? yes|no
y
Storage>

You can run other command, and you can check the defragment status by

Storage>fs list fs1
General Info:
==============
Block Size: 1024 Bytes
Version: Version 11
node_01: offline
node_02: offline

Primary Tier
============
Size: 1.00G
Use%: -
Layout: simple
Mirrors: -
Columns: -
Stripe Unit: 0.00 K
FastResync: Disabled

Mirror 1:
List of pools: pool
List of disks: disk_4 disk_5
FS Type: Normal
Defrag Status: Done successfully
Fullfsck Status: Not Running

Destroy a file system.

Storage> fs destroy fs6
100% [#] Destroy filesystem

FS
---
fs1

Set alert on the file system.

Storage> fs alert set numinodes 2M fs2
ACCESS fs SUCCESS V-288-663 Alert of type [ numinodes ] set to 2M on the file system fs2

Unset the alert on the file system.

Storage> fs alert unset numinodes fs2
ACCESS fs SUCCESS V-288-663 Alert of type [ numinodes ] set to DEFAULT value on the file system fs2

Set alert on a snapshot of the file system.
Unset the alert on a snapshot of the file system.

```
Storage> fs alert unset numinodes fs2 snap1
ACCESS fs SUCCESS V-288-663 Alert of type [numinodes] set to DEFAULT value on the file system fs2 snapshot snap1
```

Set the default alert.

```
test_01.Storage> fs alert set numinodes 2M
ACCESS fs SUCCESS V-288-663 Default Alert on the file systems of type [numinodes] set to 2M
```

Unset the default alert.

```
test_01.Storage> fs alert unset numinodes
ACCESS fs SUCCESS V-288-663 Alert of type [numinodes] set to default value 0
```

Show the alert status.

```
Storage> fs alert show
<table>
<thead>
<tr>
<th>File System</th>
<th>Alert Type</th>
<th>Value</th>
<th>Current Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs0</td>
<td>numspace</td>
<td>80% (D)</td>
<td>2%</td>
</tr>
<tr>
<td>fs0</td>
<td>numinodes</td>
<td>6500</td>
<td>1000</td>
</tr>
<tr>
<td>fs0</td>
<td>fullspace</td>
<td>98% (D)</td>
<td>2%</td>
</tr>
<tr>
<td>fs1</td>
<td>numspace</td>
<td>80% (D)</td>
<td>2%</td>
</tr>
<tr>
<td>fs1</td>
<td>numinodes</td>
<td>8000</td>
<td>10000</td>
</tr>
<tr>
<td>fs1</td>
<td>fullspace</td>
<td>98% (D)</td>
<td>2%</td>
</tr>
<tr>
<td>fs4</td>
<td>numspace</td>
<td>80(D)%</td>
<td>3%</td>
</tr>
<tr>
<td>fs4</td>
<td>numinodes</td>
<td>20000000 (D)</td>
<td>4</td>
</tr>
<tr>
<td>fs4</td>
<td>fullspace</td>
<td>98% (D)</td>
<td>3%</td>
</tr>
</tbody>
</table>
```

Upgrade the file system layout to the latest layout.

```
Storage> fs upgrade fs1
Upgrading the file system, are you sure that you want to upgrade the file system, the operation is irreversible, please enter yes/no
yes
ACCESS fs INFO V-288-2578 Proceeding with fs upgrade operation ...
ACCESS fs SUCCESS V-288-2474 file system upgraded to version 13.
```

```
Storage> fs upgrade fs1
ACCESS fs ERROR V-288-2471 File system fs1 is already at upgraded version 13.
```

```
Storage> fs upgrade fs2
ACCESS fs ERROR V-288-2482 fs2 must be online to perform upgrade operation.
```

```
Storage> fs list fs list fs1
General Info:
```
Create a schedule by name defrag_sched_1 that runs compression jobs at 11:00 pm every Saturday. This defrag job should run only for 8 hours.

Storage>fs defrag schedule create defrag_sched_1 8 15 23 * * 6
Storage>Defrag Schedule creation succeeded

Show the defrag schedule details of the schedule by name defrag_sched_1.

Storage> fs defrag schedule show defrag_sched_1
Name          Node  Duration  Minute  Hour  Day  Month  WeekDay
------------- ---- ------- -------- ----- ----- ------ -------
defrag_sched_1 any  8 hours 15  23  *  *  6

Start defrag job for file system tpcc_data1 with schedule by name defrag_sched_1.

Storage> fs defrag schedule start tpcc_data1 defrag_sched_1
Storage>starting defrag_sched_1 for fsname tpcc_data1

List the scheduled compression job status for file system tpcc_data1.

Storage> fs defrag schedule list tpcc_data1
Schedule Information for tpcc_data1
Name          Node  Duration  Minute  Hour  Day  Month  WeekDay
------------- ---- ------- -------- ----- ----- ------ -------

Create a file system for a virtual machine workload with 4 striped columns.

```
Storage> fs create pretuned vmdk_fs 100g pool1 workload=virtualmachine
    layout=striped 4
```

Create a file system for a media server workload with 8 striped columns.

```
Storage> fs create pretuned media_fs 100g pool2 workload=mediaserver layout=striped-mirror 8
```

List the file system properties of vmdk_fs.

```
storage> fs list vmdk_fs
General Info:  
=----------------------=  
Block Size: 8192 Bytes  
Version: Version 11  
Workload: virtualmachine datastore  
Extent Size: 1m  
ISAGA_01: online  
ISAGA_02: online  
Primary Tier  
=----------------------=  
Size: 100G  
Use%: 5%  
Layout: striped  
Mirrors: -  
Columns: 4  
Stripe Unit: 512 K  
Metadata: metaOk  
FastResync: Disabled
```

Create a simple file system on encrypted volume

```
Storage> fs create simple fs4 1g pool1 blksize=2048 pdir_enable=no encrypt=on
100% [#] Creating simple filesystem  
ACCESS fs SUCCESS V-288-0 Created simple file system fs4
```

Display detailed information for a specific file system

```
Storage> fs list fs4
General Info:  
=----------------------=  
Block Size: 2048 Bytes  
Version: Version 11  
Volume Encrypted: Yes  
ISA_01: online  
ISA_02: online  
Primary Tier  
=----------------------=  
Size: 1.00G  
Use%: 5%  
Layout: simple
```
Create a simple WORM enabled file system

Storage> fs create simple fs1 1g pool1 blksize=2048 pdir_enable=no encrypt=off,
     →worm=yes
100% [#] Creating simple filesystem
ACCESS fs SUCCESS V-288-0 Created simple file system fs1

Display detailed information for a specific file system

Storage> fs list fs1
General Info:
==================
Block Size: 2048 Bytes
Version: Version 13
Volume Encrypted: No
Max IOPS: 0
ISA_01: online
ISA_02: online

Primary Tier
============
Size: 1.00G
Use%: 5%
Layout: simple
Mirrors: -
Columns: -
Stripe Unit: 0.00 K
Meta Data: metaOk
FastResync: Disabled

1. Mirror 01:
List of pools: pool1
List of disks: isa_01_intel_nvme2_0

FS Type: Normal
Defrag Status: Not Running
Fullfsck Status: Not Running
Create a data movement policy policy1 for file system fs1 to move the files with file name extensions of .txt and .pdf from the primary tier (disk tier) to tier1 (cloud tier), which did not get accessed or modified for the last 2 days.

```
Storage> fs policy add operation=move policy1 fs1 primary tier1 *.txt,*.pdf atime >2d mtime >2d
ACCESS policy SUCCESS V-288-0 Policy policy1 for fs fs1 added successfully.
```

Retrieve data from Amazon Glacier. Create a policy pol1 to move all the files with file name extension of .txt from Amazon Glacier to the primary tier using the Bulk retrieval option. Files are copied to on-premises and then deleted from Amazon Glacier. The time when the files are available on-premises depends on the type of retrieval option selected.

```
Storage> fs policy add operation=move pol1 gfs2 gtier primary retrieval_option=Bulk *.txt.
```

Create a data deletion policy policy2 for file system fs1 to move the files with file name extensions of .txt and .pdf from tier1 (cloud tier), which did not get accessed or modified for the last 2 days.

```
Storage> fs policy add operation=delete policy2 fs1 tier1 \*.txt,\*.pdf atime >2d mtime >2d
ACCESS policy SUCCESS V-288-0 Policy policy2 for fs fs1 added successfully.
```

Modify data movement policy policy1 for file system fs1 to move the files with file name extension of .doc, which did not get accessed or modified for the last 3 days.

```
Storage> fs policy modify policy1 \*.doc atime >3d mtime >3d
ACCESS policy SUCCESS V-288-0 Policy policy1 modified successfully.
```

List all policies.

```
Storage> fs policy list
Name FS name Action Source Tier Destination Tier Retrieval Option Pattern Atime Mtime State
--------------- ------- ------- ------------- ------------- ------------- -------------
policy2 fs1 delete tier1 Standard \*.txt,\*.pdf >2d >2d not running
policy1 fs1 move primary tier1 Standard \*.txt,\*.pdf >2d >2d running
```

List all policies set for file system fs1.

```
Storage> fs policy list fs1
Name FS name Action Source Tier Destination Tier Retrieval Option Pattern Atime Mtime State
--------------- ------- ------- ------------- ------------- ------------- -------------
policy2 fs1 delete tier1 Standard \*.txt,\*.pdf >2d >2d running
policy1 fs1 move primary tier1 Standard \*.txt,\*.pdf >2d >2d not running
```
Delete policy policy1 set for file system fs1.

```
Storage> fs policy delete policy1 fs1
ACCESS policy SUCCESS V-288-0 Policy policy1 for fs fs1 deleted successfully.
```

Rename policy2 to policy3.

```
Storage> fs policy rename policy2 policy3
ACCESS policy SUCCESS V-288-0 Policy policy2 renamed to policy3.
```

Show the status of policy run for the policy Policy1.

```
storage> fs policy status Policy1
Policy Name: Policy1
Policy Run Type: normal
Policy Run Status: running
Total Data (Files): 93.1 GB (100000)
Moved/Deleted Data (Files): 47.7 MB (879)
Last File Visited: file100.txt
```

Abort the currently running policy Policy1.

```
storage> fs policy abort Policy1
ACCESS policy INFO V-288-0 Policy Policy1 aborted successfully.
```

Start a dry run of the policy Policy1.

```
storage> fs policy dryrun Policy1
ACCESS policy INFO V-288-0 Policy Policy1 dryrun started in background, please check 'fs policy status' for progress.
```

Pause the currently running policy Policy1

```
storage> fs policy pause Policy1
ACCESS policy INFO V-288-0 Policy Policy1 paused successfully.
```

Run the currently paused policy Policy1.

```
storage> fs policy run Policy1
Policy Policy1 is not running currently, as it was killed/paused. Would you like to start new run (y/n): y
ACCESS policy INFO V-288-0 Policy Policy1 run started in background, please check 'fs policy status' for progress.
```

Resume the currently paused policy Policy1.

```
storage> fs policy resume Policy1
ACCESS policy INFO V-288-0 Policy Policy1 resume started in background, please check 'fs policy status' for progress.
```

Create the schedule for the file system lfs1. The schedule runs every 10 minutes.

```
storage> fs policy schedule create lfs1 */10 * * * *
ACCESS policy_schedule SUCCESS V-288-0 Schedule create for file system lfs1 done successfully.
```

Modify the schedule of the file system lfs1. The schedule now runs every 20 minutes.

```
storage> fs policy schedule modify lfs1 */20 * * * *
ACCESS policy_schedule SUCCESS V-288-0 Schedule modify for file system lfs1 done successfully.
```
Veritas Access Command Reference Guide Documentation, Release 7.3

storage> fs policy schedule modify lfs1 */20 * * * *
ACCESS policy_schedule SUCCESS V-288-0 Schedule modify for file system lfs1 done successfully.

List the schedule of the file system lfs1.

storage> fs policy schedule list lfs1
File System Name  Minute  Hour  Day of Month  Month  Day of Week
=================================== =========== == =============== = == == ==
lfs1            20       *    *          *           *   *   *

Remove the schedule of the file system lfs1.

storage> fs policy schedule remove lfs1
ACCESS policy_schedule SUCCESS V-288-0 Schedule for file system lfs1 removed successfully.

Set the retention on the file /vx/myfs/file1 5y.

Storage> storage fs retention set /vx/myfs/file1 5y
ACCESS Retention SUCCESS V-288-0 Successfully set retention on /vx/myfs/file1

Set the retention on the file /vx/myfs/file1 05-20-2020.

Storage> storage fs retention set /vx/myfs/file1 05-20-2020
ACCESS Retention SUCCESS V-288-0 Successfully set retention on /vx/myfs/file1

Set the retention on the directory /vx/myfs/dir1 2y.

Storage> storage fs retention set /vx/myfs/dir1 2y
ACCESS Retention SUCCESS V-288-0 Applying retention on all current files in directory, this will take some time. Check report showevent for status.

Set the retention on the directory /vx/myfs/dir1 05-20-2020.

Storage> storage fs retention set /vx/myfs/dir1 05-20-2020
ACCESS Retention SUCCESS V-288-0 Applying retention on all current files in directory, this will take some time. Check report showevent for status.

Show the retention on the file /vx/myfs/file1

Storage> storage fs retention show /vx/myfs/file1
ACCESS Retention SUCCESS V-288-0 Retention value on file /vx/myfs/file1 is 06-08-2022 23:12:51

Show the retention on the directory /vx/myfs/dir1

Storage> storage fs retention show /vx/myfs/dir1
ACCESS Retention ERROR V-288-0 Specified path is directory path, please give file path

Clear the retention on the file /vx/myfs/file1

Storage> storage fs retention clear /vx/myfs/file1
ACCESS Retention SUCCESS V-288-0 Successfully cleared retention on /vx/myfs/file1

Clear the retention on the directory /vx/myfs/dir1
Enable worm support for specified file system.

```
Storage> fs worm set fs1
ACCESS fs SUCCESS V-288-0 Enabled WORM for fs1 file system.
```

Disable worm support for specified file system.

```
Storage> fs worm clear fs1
ACCESS fs SUCCESS V-288-0 Disabled WORM for fs1 file system.
```

### 16.7.6 SEE ALSO

disk(1), hba(1), fencing(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1) maxiops(1)
16.8 hba

16.8.1 SYNOPSIS

hba [host_name]

16.8.2 DESCRIPTION

The storage hba command displays WWN, state, and some other information for the specified node. WWN: World Wide Name State: online/offline Speed: Per Second Transmitted_FC_Frames: A value equal to the number of total transmitted Serial Attached SCSI frames across all the protocols. Received_FC_frames: A value equal to the number of total received Serial Attached SCSI frames across all the protocols. Link_Failure_Count: A value equal to the value of the LINK FAILURE COUNT field of the Link Error Status

16.8.3 EXAMPLES

Display WWN information for a particular node.

```
Storage> hba democluster_01
    HBA_Node_Name WWN                        State  Speed Support_Classes
                    --------------- ----- ----- --------------- ----
       Transmitted_FC_Frames Received_FC_frames Link_Failure_Count
                    ---------------- ------------------ ------------------
20:00:00:1b:32:89:15:5f 21:00:00:1b:32:89:15:5f offline 4_Gbit Class_3
                    445606 1815671 1
20:01:00:1b:32:a9:15:5f 21:01:00:1b:32:a9:15:5f offline unknown Class_3
                    0 0
B.Storage> democluster_01 21:00:00:1b:32:1e:5c:ba, 21:01:00:1b:32:3e:5c:ba
```

Display WWN information for all the running nodes in the cluster.

```
Storage> hba
    Node Host Initiator HBA WWNs
    ---- -----------------------
democluster_01 21:00:00:1b:32:89:15:5f, 21:01:00:1b:32:89:15:5f
         21:00:00:1b:32:a9:15:5f, 21:01:00:1b:32:a9:15:5f
         445606 1815671 1

democluster_02 21:00:00:1b:32:89:71:52, 21:01:00:1b:32:89:71:52
         21:00:00:1b:32:a9:71:52, 21:01:00:1b:32:a9:71:52
```

16.8.4 SEE ALSO

disk(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1)
16.9 iscsi

16.9.1 SYNOPSIS

iscsi status
iscsi start
iscsi stop
iscsi device add device
iscsi device del device
iscsi device list
iscsi discovery add discovery-address
iscsi discovery del discovery-address
iscsi discovery rediscover discovery-address
iscsi discovery rediscover_new discovery-address
iscsi discovery list
iscsi target add target-name portal-address
iscsi target del target-name { discovery-address | portal-address }
iscsi target login target-name { discovery-address | portal-address }
iscsi target logout target-name { discovery-address | portal-address }
iscsi target rescan target-name
iscsi target attr showdefault
iscsi target attr showall
iscsi target attr show target-name
iscsi target attr setdefault attribute value
iscsi target attr setall attribute value
iscsi target attr set target-name attribute value
iscsi target list
iscsi target listdetail target-name
iscsi initiatorname setprefix initiatorname-prefix
iscsi initiatorname list

16.9.2 TARGET ATTRIBUTES

login_timeout The amount of time the iSCSI initiator service should wait for a login to complete. The value of this attribute is in seconds. Valid values range from 10 to 600.

logout_timeout The amount of time the iSCSI initiator service should wait for logout to complete. The value of this attribute is in seconds. Valid values range from 10 to 600.
**initial_login_retry_max** The maximum number of times the iSCSI initiator should try a login to the target during the first login. This only affects the initial login. Valid values range from 1 to 16. During each login attempt wait for `login_timeout` seconds, for the login to succeed.

**noop_timeout** The amount of time the iSCSI initiator service should wait for response to a Nop-out request sent to the target, before failing the connection. Failing the connection would result in I/O to be failed and retried on any other available path. The value of this attribute is in seconds. Valid values range from 5 to 600.

**noop_interval** The time to wait between subsequent sending of Nop-out requests. The value of this attribute is in seconds. Valid values range from 5 to 600.

**replacement_timeout** The amount of time to wait for session re-establishment before failing SCSI commands. The value of this attribute is in seconds. Valid values range from 10 to 86400.

**cmds_max** The maximum number of SCSI commands the session queues. A session is defined as a connection between the initiator and the target portal for accessing a given target. `cmds_max` defines the commands per target, which could be multiple LUNs. Valid values range from 2 to 2048 and should be a power of 2.

**queue_depth** The maximum number of SCSI commands queued per LUN, belonging to a target. The value for `queue_depth` cannot be greater than `cmds_max`. Valid values range from 1 to 128.

**fast_abort** Defines whether the initiator should respond to R2Ts (Request to Transfer) after sending a task management function like an ABORT_TASK or LOGICAL UNIT RESET. A value of ‘Yes’ causes the initiator to stop responding to R2Ts after an ABORT_TASK request is received. For Equallogic arrays, the recommended value is ‘No’. Valid values are Yes/No.

### 16.9.3 OPTIONS

**device** Device on which the operation takes place.

**target-name** Name of the iSCSI target at which SCSI LUNs are available. `target-name` should conform to the naming rules defined in RFC3721.

**discovery-address** Discovery address is the target address at which the initiator can request a list of targets using SendTargets text request as specified in the iSCSI protocol of RFC3720. If no port is specified with the discovery address, the default port 3260 is used. IPv4 and IPv6 addresses are supported.

Examples:

```
192.168.0.4
192.168.0.4:3260
2001:c90::211:9ff:feb8:a9e9
[2001:c90::211:9ff:feb8:a9e9]:3260
```

**initiatorme-prefix** initiatorname-prefix is a name that conforms to the naming rules for initiator and target names as specified in RFC3721. Initiator names for nodes in the cluster are generated by appending the node number to this prefix.

**portal-address** Portal address is the location at which the target is accessible. IPv4 and IPv6 addresses are supported

Examples:

```
192.168.0.4
192.168.0.4:1
192.168.0.4:3260
192.168.0.4:3260,1
```
iscsi status Show the status of the iSCSI initiator service.

iscsi start Start the iSCSI initiator service.

iscsi stop Stops the iSCSI initiator service.

iscsi device add device Add a device for use with the iSCSI initiator. iSCSI initiator connections use this device to connect to the target. If there are any existing targets, then the iSCSI initiator initiates a connection to all the targets via device.

iscsi device del device Delete a device from the iSCSI initiator configuration. Any existing connections via device to targets are terminated. If device is the last device in the iSCSI initiator configuration and there are existing targets, then the device cannot be deleted from the configuration.

iscsi device list List the devices used by the iSCSI initiator.

iscsi discovery add discovery-address Add a discovery address to the iSCSI initiator configuration. If no TCP port is specified with the discovery-address, then the default port 3260 is used. Any targets discovered at discovery-address are automatically logged on to.

iscsi discovery del discovery-address Delete a discovery address from an iSCSI initiator configuration. Any targets discovered using discovery-address are also deleted from the configuration.

iscsi discovery rediscover discovery-address Perform a discovery of changes in targets or LUNs at discovery-address. Any LUNs or targets that have been removed at discovery-address are automatically removed from the configuration. New LUNs or targets discovered at discovery-address are automatically added and logged on to.

iscsi discovery rediscover_new discovery-address Perform a discovery of changes in targets or LUNs at discovery-address. And new LUNs or targets discovered at discovery-address are automatically added and logged on to. Does not discover any targets that have been deleted at discovery-address.

iscsi discovery list List the discovery addresses present in the iSCSI initiator configuration.

iscsi target add target-name portal-address Add a static target-portal combination to the iSCSI initiator configuration. The portal-address cannot be the same as any discovery-address present in the iSCSI initiator configuration. Connections to portal-address are made for target-name, but no discovery is done for any other targets available at portal-address. If no portal tag is specified with portal-address, the default portal tag of 1 is used.

iscsi target del target-name { discovery-address | portal-address } Delete a target target-name from the iSCSI initiator configuration. Any existing connections to target-name are terminated. discovery-address or portal-address is the address through which the target became visible to the initiator. A target that was discovered at a discovery-address once deleted from the iSCSI initiator configuration is again visible to the iSCSI initiator if re-discovery is done either through iscsi discovery rediscover or scanbus commands.

iscsi target login target-name { discovery-address | portal-address } Log on to a target target-name from the iSCSI initiator. Connections to target-name are made from all devices present in the iSCSI initiator configuration. discovery-address or portal-address is the address through which the target became visible to the initiator.

iscsi target logout target-name { discovery-address | portal-address } Log out from connections to target-name from the iSCSI initiator. discovery-address or portal-address is the address
through which the target became visible to the initiator. A target once logged out by the iSCSI initiator is not logged on to until \texttt{iscsi target login} is requested.

\textbf{iscsi target rescan target-name} Rescan target \texttt{target-name} for new LUNs.

\textbf{iscsi target attr showdefault} Show the default value for target attributes.

\textbf{iscsi target attr showall} Show the value of target attributes for all the known targets.

\textbf{iscsi target attr show target-name} Show the value of target attributes for target \texttt{target-name}

\textbf{iscsi target attr setdefault attribute value} Set the default value of \texttt{attribute} to \texttt{value}. Default value is inherited by any new targets that get added.

\textbf{iscsi target attr setall attribute value} Set the value of \texttt{attribute} to \texttt{value} for all the known targets. This does not change the default value as shown in \texttt{iscsi target attr showdefault}. Changes to the values are effective after re-login.

\textbf{iscsi target attr set target-name attribute value} Set the value of \texttt{attribute} to \texttt{value} for \texttt{target-name}. Changes to the values are effective after re-login.

\textbf{iscsi target list} List the targets visible to the iSCSI initiator. A target can be in any one of ONLINE/OFFLINE/RETRY states.

\textbf{iscsi target listdetail target-name} List detailed information about target \texttt{target-name}.

\textbf{iscsi initiatorname setprefix initiatorname-prefix} Set the prefix used to generate initiator names. Initiator names are generated as \texttt{initiatorname-prefix} followed by the node number of the node.

\textbf{iscsi initiatorname list} List the initiator names for all the nodes in the cluster.

\section*{16.9.4 EXAMPLES}

Display the status of the iSCSI initiator service.

```
Storage> iscsi status
iSCSI Initiator Status on test_1 : ONLINE
iSCSI Initiator Status on test_2 : ONLINE
```

Stop the iSCSI initiator service.

```
Storage> iscsi stop
Success.
Storage> iscsi status
iSCSI Initiator Status on test_1 : OFFLINE
iSCSI Initiator Status on test_2 : OFFLINE
```

Start the iSCSI initiator service.

```
Storage> iscsi start
Success.
Storage> iscsi status
iSCSI Initiator Status on test_1 : ONLINE
iSCSI Initiator Status on test_2 : ONLINE
```

Set the initiator name prefix used to generate the iSCSI initiator names.
Storage> iscsi initiatorname setprefix iqn.2009-05.com.test:test
Success.
Storage>

List the initiator names of all the nodes.

Storage> iscsi initiatorname list
Node Initiator Name
---- --------------
test_1  iqn.2009-05.com.test:test.1
test_2  iqn.2009-05.com.test:test.2

List the devices used by the iSCSI initiator.

Storage> iscsi device list
Device
------
pubeth0
pubeth1

Delete a device from the iSCSI initiator configuration.

Storage> iscsi device del pubeth1
100% [#] Updating disk list
Storage> iscsi device list
Device
------
pubeth0

Add a device to the iSCSI initiator configuration.

Storage> iscsi device add pubeth1
100% [#] Updating disk list
Storage> iscsi device list
Device
------
pubeth0
pubeth1

List the discovery addresses known to the iSCSI initiator.

Storage> iscsi discovery list
Discovery Address
-----------------
192.168.2.14:3260
192.168.2.15:3260

Delete a discovery address from the iSCSI initiator configuration. Any targets discovered using the discovery addresses are automatically deleted.

Storage> iscsi discovery del 192.168.2.15:3260
100% [#] Updating disk list
Storage> iscsi discovery list
Discovery Address
Add a discovery address to the iSCSI initiator configuration. Any discovered targets are automatically logged in to.

```
Storage> iscsi discovery add 192.168.2.15:3260
17% [-] Adding discovery 192.168.2.15:3260

Discovery CHAP credentials for test_1:
Outgoing CHAP Username : root
Outgoing CHAP Password : ********
Incoming CHAP Username :
Authentication succeeded.

Discovered Targets
------------------
iqn.2001-04.com.example:storage.disk5.sys3.xyz

20% [\/] Updating target configuration
Logging into target iqn.2001-04.com.example:storage.disk5.sys3.xyz

100% [#] Updating disk list
Storage> iscsi discovery list

Discovery Address
------------------
192.168.2.14:3260
192.168.2.15:3260
```

Discover changes in LUNs or targets at a discovery address already added to the iSCSI initiator configuration. Any discovered targets are automatically logged in to.

```
Storage> iscsi discovery rediscover 192.168.2.15:3260
12% [\/] Checking for deleted targets

Deleted targets
------------------
inq.2001-04.com.example:storage.disk5.sys3.xyz

Deleting iqn.2001-04.com.example:storage.disk5.sys3.xyz...done

14% [\[] Checking for new targets

New targets
------------------

100% [#] Updating disk list
```

Discover new LUNs or targets at a discovery address already added to the iSCSI initiator configuration. Any discovered targets are automatically logged in to.

```
```
Storage> iscsi discovery rediscover_new 192.168.2.15:3260
14% [ ] Checking for new targets

New targets
-------------------
100% [#] Updating disk list

Add an IPv6 discovery address.

Storage> iscsi discovery add fec0::20c:29ff:fe8e:2200
17% [-] Adding discovery fec0::20c:29ff:fe8e:2200

Discovered Targets
-------------------
iqn.2001-04.example.storage:disk.01
iqn.2002-04.example.storage:disk.02
iqn.2003-04.example.storage:disk.03
20% [ ] Updating target configuration

Logging into target iqn.2001-04.example.storage:disk.01
Logging into target iqn.2002-04.example.storage:disk.02
Logging into target iqn.2003-04.example.storage:disk.03
100% [#] Updating disk list
Storage> iscsi discovery list

Discovery Address
-------------------
[fec0::20c:29ff:fe8e:2200]:3260

Storage>

List the targets that are configured on the iSCSI initiator.

Storage> iscsi target list

<table>
<thead>
<tr>
<th>Target</th>
<th>Discovery Address</th>
<th>State</th>
</tr>
</thead>
</table>
List details of connections to a target.

Storage> iscsi target listdetail

Discovery Address : 192.168.2.14:3260

Connections
=============

<table>
<thead>
<tr>
<th>Portal Address</th>
<th>test_1</th>
<th>test_2</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.14:3260,1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Add a target using the portal address without using automatic discovery.


Storage> iscsi target listdetail iqn.2001-04.com.example:storage.disk2.sys1.xyz

Connections
=============

<table>
<thead>
<tr>
<th>Portal Address</th>
<th>test55_01</th>
<th>test55_02</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.14:3260,1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Add an IPv6 target using the portal address without using automatic discovery.

Storage> iscsi target add iqn.2001-04.ngsfellpe-04.storage:disk.01
[fec0::20c:29ff:fe8e:2200]:3260,1
100% [#] Updating disk list
Storage> iscsi target listdetail iqn.2001-04.ngsfellpe-04.storage:disk.01

Connections
=============

<table>
<thead>
<tr>
<th>Portal Address</th>
<th>test55_01</th>
<th>test55_02</th>
</tr>
</thead>
<tbody>
<tr>
<td>[fec0::20c:29ff:fe8e:2200]:3260,1</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Logout connections to a target.

100% [#] Updating disk list

Discovery Address : 192.168.2.14:3260

Connections
=============
Log on to a target.

```
100% [%] Updating disk list
```

Discovery Address : 192.168.2.14:3260

```
Connections
============
Portal Address  test_1  test_2
-------------- ----- -----  
192.168.2.14:3260,1  0    0
```

Delete a target from the iSCSI initiator configuration.

```
100% [%] Updating disk list
```

Rescan target for new LUNs.

```
100% [%] Updating disk list
Storage> iscsi target list
```

```
Target  Discovery Address  State
-----  -----------------  -----  
   Disk
------  ---------  ------ _
   ---
iqn.2001-04.com.example2:storage.disk5.sys3.xyz  192.168.2.15:3260  ONLINE  
```

Show the default value for target attributes.

```
Storage> iscsi target attr showdefault
```

```
Attribute  Value
--------  -----  
replacement_timeout  122
```
Show the value for target attributes of all known targets.

Storage> iscsi target attr showall

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>noop_timeout</td>
<td>5</td>
<td>iqn.1992-08.com.iscsi:sn.84268871</td>
</tr>
<tr>
<td>noop_interval</td>
<td>121</td>
<td>iqn.1992-08.com.iscsi:sn.84268871</td>
</tr>
<tr>
<td>queue_depth</td>
<td>32</td>
<td>iqn.1992-08.com.iscsi:sn.84268871</td>
</tr>
<tr>
<td>replacement_timeout</td>
<td>124</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>noop_timeout</td>
<td>5</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>noop_interval</td>
<td>121</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>login_timeout</td>
<td>10</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>logout_timeout</td>
<td>15</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>cmds_max</td>
<td>128</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
<tr>
<td>queue_depth</td>
<td>32</td>
<td>iqn.2009-01.com.example:storage.disk0.lun0</td>
</tr>
</tbody>
</table>

Show the value for target attributes of a given target.

Storage> iscsi target attr show iqn.1992-08.com.iscsi:sn.84268871

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>replacement_timeout</td>
<td>123</td>
</tr>
<tr>
<td>noop_timeout</td>
<td>5</td>
</tr>
<tr>
<td>noop_interval</td>
<td>121</td>
</tr>
<tr>
<td>login_timeout</td>
<td>10</td>
</tr>
<tr>
<td>logout_timeout</td>
<td>15</td>
</tr>
<tr>
<td>cmds_max</td>
<td>128</td>
</tr>
<tr>
<td>queue_depth</td>
<td>32</td>
</tr>
</tbody>
</table>

Set the default value of login_timeout to 10 seconds.

Storage> iscsi target attr setdefault login_timeout 10
Success.

Set the value of logout_timeout for all known targets to 20 seconds.

Storage> iscsi target attr setall logout_timeout 20
Changes would be applicable after next login into the target.
Success.

Set the value of noop_interval for a given target to 30 seconds.

Changes would be applicable after next login into the target.
Success.
16.9.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), quota(1)
16.10 maxiops

16.10.1 SYNOPSIS

```
fs setmaxiops " [fs_name] maxiops
fs maxioplist [fs_name]
fs iopsstat list [fs_name]
fs iopsstat reset [fs_name]
```

16.10.2 DESCRIPTION

The MAXIOPS feature enables the user to set/reset maximum I/O operations per second (MAXIOPS) value at the file system level and list/reset the maxiops statistics. When multiple applications use the same storage, it is important to balance the workload between them in a way that allows judicious use of storage resources. Setting MAXIOPS lets you control the number of input-output operations per second that storage under file system can process from an application.

16.10.3 OPTIONS

```
fs setmaxiops " [fs_name] maxiops
    set/reset MAXIOPS on a file system
fs maxioplist
    List the value of maximum I/O operations per second (MAXIOPS) set on all the file systems.
fs iopsstat list [fs_name]
    Display a statistical view of the maximum I/O operations per second (MAXIOPS) for a file system.
fs iopsstat reset [fs_name]
    Reset the MAXIOPS statistics instead of printing them.
```

16.10.4 EXAMPLES

Set maximum I/O operations per second (MAXIOPS) value for a file system fs1 to 1000:

```
Storage> fs setmaxiops fs1 1000
```

Reset maximum I/O operations per second (MAXIOPS) value for a file system fs1:

```
Storage> fs setmaxiops fs1 0
```

List maximum I/O operations per second(MAXIOPS) values for all file systems:

```
Storage> fs maxioplist

  FS                MAXIOPS
     =============== =======
    fs1 10000
    fs2 40000
```
Display statistical view of the maximum I/O operations per second (MAXIOPS) for a file system:

```
Storage> fs iopsstat list fs1
Listing IOPS stats for every 5 seconds for fs1.....
Mon Jul 10 18:14:36 IST 2017
Stats for Node test-clus_01

AVG PER SECOND VOLUMEGROUP STATISTICS
TYP NAME MaxIOPS IncomingIOPS ServicedIOPS
QueuedIOPS(Transient)
grp fs1_volgrp 20000 0 0

Stats for Node test-clus_02

AVG PER SECOND VOLUMEGROUP STATISTICS
TYP NAME MaxIOPS IncomingIOPS ServicedIOPS
QueuedIOPS(Transient)
grp fs1_volgrp 20000 0 0

Reset maximum I/O operations per second (MAXIOPS) value for a file system fs1:

```
Storage> fs iopsstat reset fs1
ACCESS fs INFO V-288-0 Resetting IOPS stats for fs1.....
ACCESS fs SUCCESS V-288-0 Sucessfully resetted the IOPS stat on all nodes
```

16.10.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), cifs(1)
16.11 pool

16.11.1 SYNOPSIS

```
pool create pool_name disk1 [, disk2,...] [isolated=yes|no]
pool adddisk pool_name disk1 [, disk2,...]
pool destroy pool_name
pool free [pool_name]
pool list
pool markdiskspare pool_name disk1 [, disk2,...]
pool removediskspare pool_name disk1 [, disk2,...]
pool mvdisk src_pool dest_pool disk1 [, disk2,...]
pool rename old_name new_name
pool rmdisk disk1 [, disk2,...]
```

16.11.2 DESCRIPTION

The storage pool command manage logical storage pools.

16.11.3 OPTIONS

- **pool create pool_name disk1 [, disk2,...] [isolated=yes|no]** Create a logical pool from a given set of disks. If isolated=yes, then a new disk group is created. The default value for isolated is isolated=no.

- **pool adddisk pool_name disk1 [, disk2,...]** Add a set of disks to a logical pool. If the disk(s) are resolved only by removing/rewriting the partition table of the disk, use `Storage>disk format disk1`.

- **pool destroy pool_name** Destroy a pool.

- **pool free [pool_name]** List free space information.

- **pool list** List all the pools.

- **pool markdiskspare pool_name disk1 [, disk2,...]** Mark a disk as a spare disk and add it to a pool which is later used for hot-relocation. In case of failure of a disk or a plex, the affected subdisks are relocated to disks designated as spare disks.

- **pool removediskspare pool_name disk1 [, disk2,...]** Remove the spare disk flag set on a disk by `markdiskspare` command.

- **pool mvdisk src_pool dest_pool disk1 [, disk2,...]** Move disks from one pool to another.

- **pool rename old_name new_name** Rename a pool.

- **pool rmdisk disk1 [, disk2,...]** Remove disks from a pool.
16.11.4 EXAMPLES

Create a pool pool1 with disks Disk_0,Disk_1.

```
Storage> pool create pool1 Disk_0,Disk_1 isolated=yes
ACCESS pool Success V-288-1015 Pool pool1 created successfully.
100% [#] Creating pool pool1
```

View the list of pools.

```
Storage> pool list
Pool  Pool Type  List of disks
====== ======== =============
pool1 Isolated  Disk_0 Disk_1
pool2 Normal   Disk_2 Disk_5
```

Destroy pool pool1.

```
Storage> pool destroy pool1
ACCESS pool SUCCESS V-288-2056 successfully destroyed the pool.
```

Remove disks from a pool.

```
Storage> pool rmdisk Disk_2
ACCESS pool Success V-288-1360 Disk(s) Disk_2 have been removed successfully.
```

Add disk Disk_2 to pool pool2.

```
Storage> pool adddisk pool2 Disk_2
ACCESS pool Success V-288-1001 Disk(s) Disk_2 are added to pool2 successfully.
```

Mark disk Disk_2 in pool2 as spare disk.

```
Storage> pool markdiskspare pool2 Disk_2
ACCESS Pool SUCCESS V-288-1360 Disk(s) Disk_2 have been marked as spared disks successfully.
```

Remove spare disk flag on Disk_2 in pool2.

```
Storage> pool removediskspare pool2 Disk_2
ACCESS Pool SUCCESS V-288-0 Disk(s) Disk_2 have been removed as spared disks successfully.
```

Rename pool1 to p01.

```
Storage> pool rename pool1 p01
ACCESS pool Success V-288-1017 Pool rename successful.
```

Move disk Disk_0 from pool p01 to pool pool2.

```
Storage> pool mvdisk p01 pool2 Disk_0
ACCESS pool Success V-288-1002 Disk(s) moved successfully.
```

View the free space in each of the pools.
View the free space in pool2.

```plaintext
Storage> pool free pool2
Disk Free Space Total Space Use%
===== =========== =========== ====
Disk_0 989.64M 989.64M 0%
Disk_2 991.69M 991.69M 0%
Disk_5 991.69M 991.69M 0%
```

16.11.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), scanbus(1), snapshot(1), tier(1), iscsi(1), quota(1)
16.12 quota

16.12.1 SYNOPSIS

quota fs enable [fs_name] [userquota | groupquota]
quota fs disable [fs_name] [userquota | groupquota]
quota fs status [fs_name] [userquota | groupquota]
quota fs set userquota | groupquota user_or_group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs setbygroup group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs show [fs_name] [userquota | groupquota] [user_or_group_names] [domain_name]
quota fs setdefault userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value] [fs_name]
quota fs showdefault [fs_name] [userquota | groupquota]
quota cifshomedir enable [userquota | groupquota] quota cifshomedir disable [userquota | groupquota] quota cifshomedir status [userquota | groupquota] quota cifshomedir set userquota | groupquota user_or_group_names domain_name [hardlimit | softlimit] [numinodes | numspace] [value] quota cifshomedir setall userquota | groupquota [hardlimit | softlimit] [numinodes | numspace] [value] quota cifshomedir show [userquota | groupquota] [user_or_group_names] [domain_name] quota cifshomedir showdetail [userquota | groupquota] [user_or_group_names] [domain_name] quota cifshomedir setdefault userquota | groupquota hardlimit | softlimit numinodes | numspace [value] quota cifshomedir showdefault [userquota | groupquota]

16.12.2 DESCRIPTION

The storage quota commands are for configuring disk quotas on file systems for users and groups. There are two types of disk quotas, one is a usage quota (numspace), and the other is an inode quota (numinodes). A quota limit can be set as a soft quota limit (soflimit) where users are warned against exceeding the quota limits, and there is a grace period during which the user is allowed to exceed the quota limits. After the grace period is over, the user is not allowed to exceed the quota limits. Hard quota limits (hardlimit) can also be set so that the user is not allowed to exceed the quota limits. The soflimit has to be less than the hardlimit for any type of quota.

The storage quota fs commands are for configuring quotas on file systems that are not part of the CIFS home directories. The storage quota cifshomedir commands are for configuring quotas on CIFS home directories. All users and groups visible through different sources of Name Service Lookup (nsswitch), such as, local users, LDAP, NIS, Windows users, and so on, can be configured for quotas.

16.12.3 OPTIONS

quota fs enable [fs_name] [userquota | groupquota]
quota cifshomedir enable [userquota | groupquota]

Enable user or group quota on a file system or CIFS home directories.
quota fs disable [fs_name] [userquota|groupquota]
quota cifshomedir disable [userquota|groupquota]

Disable user or group quota on a file system or CIFS home directories.

quota fs status [fs_name] [userquota|groupquota]
quota cifshomedir status [userquota|groupquota]

Show the status of quota settings on a file system or CIFS home directories. This only shows if the quota is enabled or disabled.

quota fs set userquota | groupquota user_or_group_names domain_name [hardlimit|softlimit] [numinodes|numspace] [value] [fs_name]
quota cifshomedir set userquota | groupquota user_or_group_names domain_name [hardlimit|softlimit] [numinodes|numspace] [value]

Set a quota value for users or groups on a file system or CIFS home directories. If value is not specified, then the default value set from the respective setdefault commands is used to configure the quota limit. If value is 0, it is treated as unlimited quota. If all values of user or group quota are 0, the user or group is automatically deleted from the quota settings, which means quota fs status does not show this user’s or group’s settings, as all quota values are unlimited for it.

quota fs setall userquota | groupquota [hardlimit|softlimit] [numinodes|numspace] [value] [fs_name]
quota cifshomedir setall userquota | groupquota [hardlimit|softlimit] [numinodes|numspace] [value]

Set quota value for all users and groups for whom the quota has already been set with set commands. Other users and groups (for whom quota has not been set previously) are not affected. If value is not specified, then the default value set from the respective setdefault commands is used to configure the quota limit. If value is 0, it is treated as an unlimited quota. If all values of user or group quota are 0, the user or group are automatically deleted from the quota settings, which means quota fs status does not show this user’s or group’s settings, as all quota values are unlimited for it.

quota fs setbygroup group_names domain_name [hardlimit|softlimit] [numinodes|numspace] [value] [fs_name]

Set the user quota for users of specified groups.

quota fs show [fs_name] [userquota|groupquota] [user_or_group_names] [domain_name]
quota cifshomedir show [userquota|groupquota] [user_or_group_names] [domain_name]
quota cifshomedir showdetail [userquota|groupquota] [user_or_group_names] [domain_name]

Show the quota values that are already set. This also shows the consumed (used space) quota of users and groups. cifshomedir show shows the general quota values on the CIFS home directories. cifshomedir showdetail shows the detailed quota values set on each file system for CIFS home directories.

quota fs setdefault userquota | groupquota hardlimit|softlimit numinodes|numspace [value] [fs_name]
quota cifshomedir setdefault userquota | groupquota hardlimit|softlimit numinodes|numspace [value]

Set the default value that is used for quota limits. The values are put in a configuration file only. The actual application of quotas can be done with set and setall commands using these default values.
quota fs showdefault [fs_name] [userquota | groupquota]
quota fs showdefault [userquota | groupquota]

Show the default quota values from the configuration file.

16.12.4 EXAMPLES

Enable quota (user and group quota) for file system fs1:

```
Storage> quota fs enable fs1
OK Completed
```

Enable quota (user and group quota) for CIFS home directories:

```
Storage> quota cifshomedir enable
OK Completed
```

Disable userquota for file system fs1:

```
Storage> quota fs disable fs1 userquota
OK Completed
```

Disable groupquota for CIFS home directories:

```
Storage> quota cifshomedir disable groupquota
OK Completed
```

Show status of file system quota (enabled or disabled):

```
Storage> quota fs status
 FS name     User Quota Group Quota
========     =========== ===========
 fsmirror    Disabled   Disabled
 quotasfs    Enabled    Enabled
 striped1    Enabled    Enabled
 fs1         Disabled   Enabled
 OK Completed
```

Show status of CIFS home directory quota (enabled or disabled):

```
Storage> quota cifshomedir status
 FS name         User Quota Group Quota
========         =========== ===========
 CIFS homedirectories    Enabled   Disabled
 OK Completed
```

Set userquota (hardlimit and numinodes) of user qtuser on file system fs1:

```
Storage> quota fs set userquota qtuser qtdomain hardlimit numinodes 957 fs1
OK Completed
Storage> quota fs show fs1 userquota qtuser qtdomain
User quota details for file system fs1:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Space Used</th>
<th>Soft Space</th>
<th>Hard Space</th>
<th>Inodes Used</th>
<th>Soft Inodes</th>
<th>Hard Inodes</th>
</tr>
</thead>
</table>
```

Chapter 16. Storage Commands
Set user quota (hardlimit and numinodes) of user qtuser on CIFS home directories:

```bash
Storage> quota cifshomedir set userquota qtuser qtdomain hardlimit numinodes 6549
OK Completed
```

User quota details for CIFS home directories:

```bash
User Name   Space Used  Soft Space  Hard Space  Inodes Used  Soft Inodes
----------   ----------  ----------  ----------  ----------  ----------
qtdomain\qtuser 0          20M        100M       0           1000
       6549
```

Set all existing user quotas to default values:

```bash
Storage> quota fs setall userquota
OK Completed
```

Set all existing user quotas for CIFS home directories:

```bash
Storage> quota cifshomedir set userquota qtuser qtdomain hardlimit numinodes 6549
OK Completed
```

User quota details for CIFS home directories:

```bash
User Name   Space Used  Soft Space  Hard Space  Inodes Used  Soft Inodes
----------   ----------  ----------  ----------  ----------  ----------
qtdomain\qtuser 0          20M        100M       0           1000
       6549
```

User quota details for file system fs1:

```bash
User Name   Space Used  Soft Space  Hard Space  Inodes Used  Soft Inodes
----------   ----------  ----------  ----------  ----------  ----------
a1           0          0            10G         0           1000
       10000
qtuser       0          0            0           0           0
       957
qtuser2      0          1000K       0           0           0
```

Set all existing user quotas to default values:

```bash
Storage> quota fs setall userquota
OK Completed
```

Set all existing user quotas for CIFS home directories:

```bash
Storage> quota cifshomedir set userquota qtuser qtdomain hardlimit numinodes 6549
OK Completed
```

User quota details for CIFS home directories:

```bash
User Name   Space Used  Soft Space  Hard Space  Inodes Used  Soft Inodes
----------   ----------  ----------  ----------  ----------  ----------
qtdomain\qtuser 0          20M        100M       0           1000
       6549
```
Storage> quota cifshomedir show

User Name   | Space Used | Soft Space | Hard Space | Inodes Used | Soft Inodes | Hard Inodes |
-------------|------------|------------|------------|-------------|-------------|-------------|
qtuser       | 0          | 20M        | 100M       | 0           | 1000        | 6549        |

OK Completed

Storage> quota cifshomedir setall userquota softlimit numinodes 198
OK Completed

Storage> quota cifshomedir show

User quota details for CIFS home directories:

User Name   | Space Used | Soft Space | Hard Space | Inodes Used | Soft Inodes | Hard Inodes |
-------------|------------|------------|------------|-------------|-------------|-------------|
qtuser       | 0          | 20M        | 100M       | 0           | 198         | 6549        |

OK Completed

Set user quotas for users of specified groups.

Storage> quota fs setbygroup cifsgroup1 local softlimit numspace 50M fs1
OK Completed

Storage> quota fs show

User quota details for file system fs1:

User Name   | Space Used | Soft Space | Hard Space | Inodes Used | Soft Inodes | Hard Inodes |
-------------|------------|------------|------------|-------------|-------------|-------------|
cifsuser1    | 0          | 50M        | 0          | 0           | 0           | 0           |
cifsuser2    | 0          | 50M        | 0          | 0           | 0           | 0           |

OK Completed

Show file system quota values:

Storage> quota fs show

User quota details for file system quotafs:

User Name   | Space Used | Soft Space | Hard Space | Inodes Used | Soft Inodes | Hard Inodes |
-------------|------------|------------|------------|-------------|-------------|-------------|
quotauser    | 10M        | 1M         | 20M        | 1           | 5           |             |
quotauser    | 9M         | 1M         | 10M        | 1           | 0           |             |
qtuser       | 10M        | 10M        | 20M        | 9           | 5           |             |
qtuser2      | 19M        | 5M         | 20M        | 1           | 0           |             |

OK Completed
User quota details for file system fs1:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Space Used</th>
<th>Soft Space</th>
<th>Hard Space</th>
<th>Inodes Used</th>
<th>Soft Inodes</th>
<th>Hard Inodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>0</td>
<td>0</td>
<td>10G</td>
<td>0</td>
<td>1000</td>
<td></td>
</tr>
<tr>
<td>qtuser</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>qtuser2</td>
<td>0</td>
<td>1000K</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

User quota details for file system longfilesystemnameforqt:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Space Used</th>
<th>Soft Space</th>
<th>Hard Space</th>
<th>Inodes Used</th>
<th>Soft Inodes</th>
<th>Hard Inodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>qtuser</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>901</td>
<td></td>
</tr>
</tbody>
</table>

OK Completed

Show CIFS home directory quota values:

Storage> quota cifshomedir show

User quota details for CIFS home directories:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Space Used</th>
<th>Soft Space</th>
<th>Hard Space</th>
<th>Inodes Used</th>
<th>Soft Inodes</th>
<th>Hard Inodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>qtuser</td>
<td>0</td>
<td>20M</td>
<td>100M</td>
<td>0</td>
<td>198</td>
<td></td>
</tr>
</tbody>
</table>

OK Completed

Set default group quota value:

Storage> quota fs setdefault groupquota hardlimit numspace 1T
OK Completed

Set default CIFS home directory user quota value:

Storage> quota cifshomedir setdefault userquota hardlimit numspace 2T
OK Completed

Show default quota values:

Storage> quota fs showdefault

Default quota values:

<table>
<thead>
<tr>
<th>Title</th>
<th>Hard Inodes</th>
<th>User/Group Quota</th>
<th>Soft Space</th>
<th>Hard Space</th>
<th>Soft Inodes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16.12. quota
Default Quota  User Quota  -  -  -  -  -  -
  →  1000
Default Quota  Group Quota  -  1T  -  -  -  -
  →  -

Per FS default quota values:

FS Name  User/Group Quota  Soft Space  Hard Space  Soft Inodes  Hard Inodes
  →  Hard Inodes
  →  ===============  ================  ==========  ===========  ===========  ===========
  →  fs1  User Quota  -  -  -  -  -
  →  1000
OK Completed

Show default CIFS home directory quota values:

Storage> quota cifshomedir showdefault
CIFS homedir default quota values:

User/Group Quota  Soft Space  Hard Space  Soft Inodes  Hard Inodes
  →  ===============  ================  ==========  ===========  ===========
  →  User Quota  -  2T  -  -
  →  Group Quota  -  -  -  -
OK Completed

16.12.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), cifs(1)
16.13 rollback

16.13.1 SYNOPSIS

rollback create space-optimized rollback_name fs_name [cacheobj]
rollback create full-sized rollback_name fs_name pool
rollback restore fs_name rollback_name
rollback refresh rollback_name fs_name
rollback destroy rollback_name fs_name
rollback list [fs_name/rollback_name]
rollback online rollback_name fs_name
rollback offline rollback_name fs_name
rollback cache create cache_name [cache_size] [pool]
rollback cache destroy cache_name
rollback cache list [cache_name]
rollback cache growby cache_name cache_size
rollback cache growto cache_name cache_size

16.13.2 DESCRIPTION

The storage rollback commands manage volume-level snapshots. All rollback commands take a file system as an argument and perform operations on the underlying volume of that file system.

Both space-optimized and full-sized rollbacks are supported. Space-optimized rollbacks use a storage cache and do not need a complete copy of the original volume’s storage space. However, space-optimized rollbacks are not suitable for write-intensive volumes, because the copy-on-wirte mechanism may degrade the performance of the volume. Full-sized rollbacks use more storage, but it has little impact on write performance after synchronization is completed.

The rollback command can be used to perform the following operations:

• Creating/destroying/listing instant rollbacks for a given file system.
• Restoring a file system by a given instant rollback.
• Refreshing an instant rollback from a file system.
• Onlining/offlining instant rollbacks for a given file system.
• Creating/destroying/listing cache object that can be used for instant rollbacks.

16.13.3 OPTIONS

rollback create space-optimized rollback_name fs_name [cacheobj] Create a space-optimized rollback for a specified file system. If the cacheobj is specified, then the shared cache object is used. Or the system automatically creates a cache object for the rollback.

rollback create full-sized rollback_name fs_name pool Create a full-sized rollback for a specified file system. The disks used for the rollback are allocated from the specified pool.

rollback restore fs_name rollback_name Restore a file system by a given rollback.
rollback refresh rollback_name fs_name  Refresh an instant rollback from a file system.

rollback destroy rollback_name fs_name  Destroy the instant rollback of a file system.

rollback list [fs_name/rollback_name]  Display all the instant rollbacks of the specified file system. If rollback name is specified, then display information about the specified rollback. If no file system name or rollback name is specified, then instant rollbacks of all the file systems are displayed.

rollback online rollback_name fs_name  Place the instant rollback online.

rollback offline rollback_name fs_name  Place the instant rollback offline.

rollback cache create cache_name [cache_size] [pool]  Create a shared cache object or convert the file system to a shared cache object for space-optimized rollbacks for the file system. If cache_size and pool are both specified, create a shared cache object. If only cache_name is specified, convert the file system to a shared cache object. cache_name should be the same as an existing file system name that is to be converted. There is a confirmation message in the Veritas Access CLI asking if you want to convert the specified file system to a cache object.

rollback cache destroy cache_name  Destroy the shared cache object.

rollback cache list [cache_name]  Display the shared cache objects. If no cache_name is specified, all cache objects are displayed. The disabled cache object is listed with ‘-’ as the attribute. If cache_name is specified and the cache object is disabled, the cache object is enabled automatically.

rollback cache growby cache_name cache_size  Grow the size of the cache object by a specified amount. The cache size should be specified in terms of 512 bytes unit. To calculate the cache size, convert the cache size that you want in KB and multiply by 2.

rollback cache growto cache_name cache_size  Grow the size of the cache object to a specified amount. The cache size should be specified in terms of 512 bytes unit. To calculate the cache size, convert the cache size that you want in KB and multiply by 2.

16.13.4 EXAMPLES

Create a space-optimized rollback of a file system.

Storage> rollback create space-optimized snap4 fs4
100% [%] Create rollback

Create a full-sized rollback of a file system.

Storage> rollback create full-sized snap5 fs4 pool1
100% [%] Create rollback

Restore a file system by a given instant rollback.

Storage> rollback restore fs4 snap4

Destroy the instant rollback of a file system.

Storage> rollback destroy snap4 fs4
100% [%] Destroy rollback
View the list of instant rollbacks.

```
Storage> rollback list
NAME       TYPE     FILESYSTEM SNAPDATE
roll15     fullinst fs4        2010/10/15 20:04
roll11     spaceopt bigfs     2010/10/15 17:03
```

View the list of instant rollbacks.

```
Storage> rollback list fs4
NAME       TYPE     SNAPDATE          CHANGED_DATA  SYNCED_DATA
roll15     fullinst 2010/10/15 20:04  640K(0.1%)  800M(100%)
```

Create a shared cache object.

```
Storage> rollback cache create cobj1 100m pool1
100% [#]
```

Convert the file system to a shared cache object.

```
Storage> rollback cache create fs_to_cache
ACCESS rollback WARNING V-288-0 Filesystem fs_to_cache will be converted to cache_object. All data on Filesystem fs_to_cache will be lost
ACCESS rollback WARNING V-288-0 Are you sure to convert fs_to_cache to cache object?
(yes/no)
yes
100% [#]
```

Grow the size of the cache object by a specified amount. In following example, the cache size is grown by 1M.

```
Storage> rollback cache growby cobj1 2048
ACCESS rollback SUCCESS V-288-0 Size of cache object cobj1 extended successfully.
```

Grow the size of the cache object to a specified amount. In following example, the cache size is grown to 10G.

```
Storage> rollback cache growto cobj1 20971520
ACCESS rollback SUCCESS V-288-0 Size of cache object cobj1 extended successfully.
```

Display the shared cache object.

```
Storage> rollback cache list
CACHE NAME TOTAL(Mb) USED(Mb) (%) AVAIL(Mb) (%) SDCNT
fs_cache1   10 4 (40)   6 (60)   0
cache2      - - - - -
```

```
Storage> rollback cache list cache2
rollbacks located on cache cache2:
roll12
```

```
Storage> rollback cache list cache_disabled
rollbacks located on cache cache_disabled:
roll13
ACCESS rollback WARNING V-288-0 Cache object cache_disabled was DISABLED, trying to restart it.
ACCESS rollback INFO V-288-0 Cache object cache_disabled started successfully.
```

16.13. rollback
16.13.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), tier(1), iscsi(1), quota(1)
16.14 scanbus

16.14.1 SYNOPSIS

scanbus [ force ]

16.14.2 DESCRIPTION

The storage scanbus command scans all the SCSI devices connected to all the nodes of the cluster. It scans the disks on all the nodes without interrupting existing I/O activity, and it updates the configuration. It does not inform the user even if there is a change in the storage configuration. Users can see the latest storage configuration with the disk list command.

16.14.3 OPTIONS

force Tries to import pools forcefully. This may help when normal scanbus alone fails.

16.14.4 EXAMPLES

Scan SCSI Bus for newly added disks.

Storage> scanbus
100% [#] Scanning the bus for disks

16.14.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), snapshot(1), tier(1), iscsi(1), quota(1)
16.15 snapshot

16.15.1 SYNOPSIS

snapshot create snapshot_name fs_name [removable=yes|removable=no]
snapshot restore snapshot_name fs_name
snapshot destroy snapshot_name fs_name
snapshot list [fs_name] [schedule_name]
snapshot online snapshot_name fs_name
snapshot offline snapshot_name fs_name
snapshot quota on [fs_name] [capacity_limit]
snapshot quota off [fs_name] [remove_limit]
snapshot quota list
snapshot schedule create schedule_name fs_name max_snapshot_limit minute [hour]
 [day_of_the_month] [month] [day_of_the_week] [max_num_of_no_named_fset]
snapshot schedule modify schedule_name fs_name max_snapshot_limit minute [hour]
 [day_of_the_month] [month] [day_of_the_week] [max_num_of_no_named_fset]
snapshot schedule destroyall schedule_name fs_name
snapshot schedule preserve schedule_name fs_name snapshot_name
snapshot schedule show fs_name [schedule_name]
snapshot schedule delete fs_name [schedule_name]

16.15.2 DESCRIPTION

The storage snapshot commands manage file system level snapshots. All snapshot commands take a file system as an argument and perform operations on that file system.

The snapshot command can be used to perform the following:

• Adding/removing/destroying/listing snapshots for a given file system.
• Restoring a file system by a given snapshot.
• Onlining/offlining snapshots for a given file system.
• Turning on/off quota value for the space that can be utilized for snapshot creation corresponding to a given file system name.
• Creating/modifying a schedule that automatically creates snapshots for a given file system every X hours and Y minutes.
• Destroying all automated snapshots corresponding to a given schedule name and file system name. If any snapshot is preserved or online, the command fails.
• Preserving an automated snapshot so that it is not automatically removed once the command snapshot schedule autoremove has been run.
• Displaying/deleting schedules created for automated snapshot creation and removal.
Automated snapshot creation

A snapshot can be created in two ways: either manually using the `snapshot create` command, or by creating a schedule that calls the `snapshot create` command periodically depending on the values entered for the number of hours or minutes after which this command should be run. (Notice: We suggest to only create one schedule for a specified file system, otherwise `storage snapshot schedule destroyall` may take a long time).

Thus a key feature of the `snapshot` command is to allow for creation of a schedule that can create a snapshot in an automated manner. This is done by storing the values for minute, hour, day-of-month, month, and day-of-week in the crontab along with the name of the file system for which the snapshot is created automatically. To distinguish the automated snapshots, a timestamp corresponding to their time of creation is appended to the schedule name. Thus a snapshot created under schedule1 on 27th February 2009 at 11 am is named as:

```
schedule1_Feb_27_2009_11_00_01_IST
```

The following are the main parameters and the type of values one can provide while creating or modifying a schedule for automated snapshot creation:

1. **Schedule name:** This specifies the name of the schedule corresponding to which a snapshot is created automatically. The schedule name cannot contain an underscore `_` as part of its input value. This is by design. So a schedule name such as `s_1` is not allowed.

2. **Max Snapshot Limit:** This specifies the number of snapshots that can be created for a given file system and schedule name. This field accepts numeric input only. The range of this value is from ‘1’ to ‘366’. This value would imply that only x number of snapshots can be created for a given file system and schedule name. If the number of snapshots corresponding to a schedule name is equal to or greater than the value of this field, then snapshots are automatically destroyed till the number of snapshots is less than the maximum snapshot limit value.

3. **Minute:** This field may contain either an asterisk like `*/15`, which implies every 15 minutes. (Notice: If using ‘xx’ format, the smallest value for ‘xx’ is 15) or a numeric value between 0-59.

4. **Hour:** This field may contain either an asterisk `*`, which implies every hour, or a numeric value between 0-23.

5. **Day of month:** This field may contain either an asterisk `*`, which implies every day of the month, or a numeric value between 1-31.

6. **Month:** This field may contain either an asterisk `*`, which implies run every month, or a numeric value between 1-12. In addition to the numeric values, this field can also accept names of month as arguments, with the first three letters of the month (all in lowercase) serving as input for the given parameter.

7. **Day of Week:** This field may contain either an asterisk `*`, which implies every day of the week, or a numeric value between 0-6, with 0 being interpreted as Sunday, 1 as Monday and so on. In addition, this parameter can also accept names, with the first three letters of the month (all in lowercase) serving as input values.

8. **Number of maximum removing no named fset:** This field has a default value of 2, which implies that if the current removing no-named-fset exceeds that value, successive snapshot auto-create can be skipped.

**Note:**

1. By default, the parameters hour, day-of-month, month, and day-of-week for `snapshot schedule create` command contain a `*` or an asterisk value, while `max_num_of_no_named_fset` is set to 2 by default as they are all optional arguments.

2. The parameters minute, hour, day-of-month, month, and day-of-week for `snapshot schedule create` and `snapshot schedule modify` can accept numeric values in the form of ranges, where a range is defined as two numbers separated by a hyphen. So if one wishes to run the schedule between 1 am and 4 am, then one can specify a value 1-4 for 'hour' parameter, with the range being inclusive.

3. Similarly, one can specify a step value for other parameters, that is, day-of-month, month, and day-of-week as well. Step values are also allowed after an asterisk `*`, so if one wishes to run a schedule every two hours, one just has to specify `*/2` as the input value for the 'hour' parameter.
4. The range of value max_num_of_no_named_fset is from 2 to 5.

So to create a snapshot every two and half hours with at most 50 snapshots per schedule name with a maximum of 4 removing no-named-fsets, you have to run the following command:

```
snapshot schedule create sched1 fs1 50 */30 */2 * * * 4
```

### 16.15.3 OPTIONS

**snapshot create snapshot_name fs_name** [removable=yes|removable=no]

Create a snapshot for a specified file system. If the removable attribute is yes and if it is offline, then it is removed automatically, if the file system runs out of space.

**snapshot restore snapshot_name fs_name**

Restore a file system by a given snapshot.

**snapshot destroy snapshot_name fs_name**

Destroy the snapshot of a file system.

**snapshot list [fs_name] [schedule_name]**

Display all the snapshots of the specified file system and schedule name. If no file system is specified, snapshots of all the file systems are displayed, whereas if no schedule_name is specified, then snapshots created under fs_name are displayed.

**snapshot online snapshot_name fs_name**

Place the snapshot online.

**snapshot offline snapshot_name fs_name**

Place the snapshot offline.

**snapshot quota on fs_name [capacity_limit]**

Disallow creation of snapshots on the given file system when the space used by all the snapshots of that file system exceeds a given capacity limit.

**snapshot quota off [fs_name] [remove_limit]**

Disable quota capacity limit for a specified system. The default remove_limit value is true. If it is false, the capacity limit is not reset.

**snapshot quota list**

Display snapshot quota information of all the file systems.

**snapshot schedule create schedule_name fs_name max_snapshot_limit minute** [hour] [day_of_the_month] [month] [day_of_the_week] [max_num_of_no_named_fset]

Create a schedule for automated snapshot creation of a particular file system.

**snapshot schedule modify schedule_name fs_name max_snapshot_limit minute** [hour] [day_of_the_month] [month] [day_of_the_week] [max_num_of_no_named_fset]

Modify the schedule for automated snapshot creation of a particular file system.

**snapshot schedule destroyall schedule_name fs_name**

Destroy all automated snapshots corresponding to a given schedule name and file system name. If any snapshot is preserved or online, the command fails.

**snapshot schedule preserve schedule_name fs_name snapshot_name**
Preserve a limited number of snapshots corresponding to an existing schedule and a specific file system name so that they are not removed as part of the snapshot schedule autoremove command.

```
snapshot schedule show fs_name [schedule_name]
```

Show all schedules that have been set for automated snapshot creation.

```
snapshot schedule delete fs_name [schedule_name]
```

Delete the schedule set for automated snapshot creation for a particular file system or for a particular schedule.

### 16.15.4 EXAMPLES

Create a snapshot of a file system.

```
Storage> snapshot create snapshot1 fs1
100% [#] Create snapshot
```

Restore a file system by a given snapshot.

```
Storage> snapshot restore snapshot1 fs1
```

Destroy the snapshot of a file system.

```
Storage> snapshot destroy snap1 fs1
100% [#] Destroy snapshot
```

View the list of snapshots.

```
Storage> snapshot list
Snapshot Schedule Name Status ctime
--- ------- ========= ======
-02009.Jul.27.02:40:57 no no 190.0M
-02009.Jul.24.21:34:03 yes no 900.0M
-02009.Jul.24.19:34:04 yes no 7.0G
-02009.Jul.24.18:34:04 yes yes 125M
-02009.Jul.24.17:34:04 yes no 0K
```

Display the list of snapshots for a given file system.

```
Storage> snapshot list fs2
Snapshot Schedule Name Status ctime
--- ------- ========= ======
-02009.Jul.27.02:40:57 yes no 190.0M
-02009.Jul.24.22:34:09 yes no 900.0M
-02009.Jul.24.21:34:03 yes no 7.0G
```
Display the list of snapshots corresponding to a file system and schedule name.

```
Storage> snapshot list fs1 scl
Snapshot Status ctime mtime
--- --------------- ----- ----- ----
```

Make a snapshot offline.

```
Storage> snapshot offline snapshot1 fs1
100% [#] Offline snapshot
```

Make a snapshot online.

```
Storage> snapshot online snapshot1 fs1
100% [#] Online snapshot
```

Enable the snapshot quota of a file system.

```
Storage> snapshot quota on fs1
Storage> snapshot quota on fs1 1M
```

Disable the snapshot quota of a file system.

```
Storage> snapshot quota off fs2
Storage> snapshot quota off fs3 true
Storage> snapshot quota off fs4 false
Storage> snapshot quota off fs5
```

Display the list of snapshot quotas of all the file systems.

```
Storage> snapshot quota list
FS                      Quota Capacity Limit
------------------------ ------ ---------------
fs1                      on    1M
fs2                      off    0
fs3                      off    0
fs4                      off    1M
fs5                      off    0
```
Create a schedule for automated snapshot creation of a given file system every 3 hours on a daily basis and only 30 snapshots can be treated for a given schedule, and the maximum removing no-named-fset is 3.

```
Storage> snapshot schedule create schedule1 fs1 30 * 3 * * * 3
```

Modify the existing schedule so that the snapshot is created every 2 hours on the first day of the week, and only 20 snapshots can be created for a given schedule.

```
Storage> snapshot schedule modify schedule1 fs1 20 * 2 * * 1
```

Destroy all automated snapshots created under a given schedule and file system.

```
Storage> snapshot schedule destroyall schedule1 fs1
```

Preserve a snapshot created according to a given schedule and file system name.

```
Storage> snapshot schedule preserve schedule1 fs1 schedule1_Feb_27_16_42_00_IST
```

List all schedules created for automated snapshot creation corresponding to an existing file system.

```
Storage> snapshot schedule show fs3
```

<table>
<thead>
<tr>
<th>FS</th>
<th>Schedule Name</th>
<th>Max Snapshot</th>
<th>Minute</th>
<th>Hour</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs3</td>
<td>sched1</td>
<td>30</td>
<td>*/20</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>fs3</td>
<td>sched2</td>
<td>20</td>
<td>*/45</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

List automated snapshot schedules for all file systems.

```
Storage> snapshot schedule show
```

<table>
<thead>
<tr>
<th>FS</th>
<th>Schedule Name</th>
<th>Max Snapshot</th>
<th>Minute</th>
<th>Hour</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs6</td>
<td>sc1</td>
<td>10</td>
<td>*/50</td>
<td>*</td>
<td>*</td>
</tr>
<tr>
<td>fs1</td>
<td>sc1</td>
<td>10</td>
<td>*/25</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

Delete all schedules created for automated snapshot creation or removal corresponding to an existing file system.

```
Storage> snapshot schedule delete fs1
```

### 16.15.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), tier(1), iscsi(1), quota(1)
16.16  tier

16.16.1  SYNOPSIS

tier add cloud fs_name tier_name service_name region S3|Glacier
tier add simple fs_name size pool1 [, disk1,...]
 tier add mirrored fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool]
 tier add striped fs_name size ncolumns pool1 [, disk1,...] [stripeunit=<kilobytes>]
 tier add mirrored-stripe fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>]
 tier add striped-mirror fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripeunit=<kilobytes>]
 tier addcolumn fs_name ncolumns pool1 [, disk1,...]
 tier rmcolumn fs_name
 tier remove fs_name [tier_name]
 tier list fs_name
 tier move start fs_name source_tier destination_tier retrieval_option=Expedited|Standard|Bulk pattern [atime|mtime] [atime|mtime]
 tier move list
 tier move status JOBID
 tier move abort JOBID
 tier move dryrun fs_name source_tier destination_tier pattern [atime|mtime] [atime|mtime]
 tier addmirror fs_name pool1 [, disk1,...] [protection=disk|pool]
 tier rmmirror fs_name [pool_or_disk_name]
 tier listfiles fs_name {primary|secondary}
 tier mapfile fs_name file_path
 tier policy list
 tier policy prune list
 tier policy prune modify fs_name delete_after
 tier policy modify fs_name {primary|secondary} days minacctemp period
 tier relocate fs_name dirPath
 tier policy remove fs_name
 tier policy prune remove fs_name
 tier policy run fs_name
 tier schedule list
 tier schedule modify fs_name minute hour day_of_the_month month day_of_the_week node_name
 tier schedule remove fs_name
 tier query fs_name
tier allowmetadata yes fs_name

 tier allowmetadata no fs_name

 tier setfastresync fs_name pool1 [, disk1,...]

 tier unsetfastresync fs_name

 tier stats monitor fs_name tier_name [interval]

 tier stats {show|reset|usage} fs_name tier_name

16.16.2 DESCRIPTION

Veritas Access provides two types of tiers, a primary tier and a secondary tier. Each created file system will have only one primary tier initially. This tier cannot be removed. Operations like fs addmirror, fs growto primary, fs shrinkto primary, and so on, will be applied to the primary tier.

Veritas Access includes a feature, cloud as a tier, that lets you move files based on user-specified criteria to cloud storage. This feature is supported for scale-out file systems only. Based on the criteria specified for data movement using the storage tier move operation, data is moved to and from the cloud automatically.

The storage tier commands manage file system secondary tiers. All tier commands take a file system name as an argument and perform operations on the secondary tier of that file system.

A file system cannot have more than one tier of the same type.

The tier command can be used to perform the following:

• adding/removing/modifying the secondary tier
• adding/removing the cloud tier for scale-out file systems
• adding/removing an S3-compatible or Amazon Glacier cloud tier
• moving files between the primary tier and the cloud tier for scale-out file systems
• listing storage tiers configured for scale-out file systems
• setting policies
• scheduling policies
• locating tier locations of files
• listing files that are located on the primary or the secondary tier
• listing the tier type as S3 or Amazon Glacier
• moving files from the secondary tier to the primary tier

Policy:

Each tier can be assigned a policy. A policy assigned to a file system has three parts:

1. File Creation This specifies on which tier new files get created.

2. Inactive files This indicates when a file has to be moved from the primary tier to the secondary tier and can be determined by observing the files’ last modification date instead of the last accessed date. For example, if the days of a tier is set to 10 days, and if file1 has not been modified for the last 10 days, while file2 has been modified in between, then only file1 will be moved to the secondary tier, whereas file2 still remains in the primary tier.
3. **Access Temperature** Access temperature is the measure of the number of I/O requests to the file during the period designated by the period. In other words, access temperature is the number of read or write requests made to a file over a specified number of 24-hour periods divided by the number of periods. So if the access temperature of a file exceeds more than minacctemp (where the access temperature is calculated over a period specified by period), then this file is moved from the secondary tier to the primary tier.

**Schedule:**

When a file is not accessed for more than policy number of days, then it is not moved automatically from one tier to another tier. This movement has to be scheduled manually. This schedule has to be set for each file system.

For example, if the user sets the schedule as “0 0 2 * *”, and the policy as 60, then on the 2nd of every month, all the files that have not been accessed for more than 60 days are moved from the primary tier to the secondary tier.

The following are the parameters that you can provide while setting a schedule for moving a file from the primary to the secondary tier:

1. File system name: File system whose files are to be moved from the primary to a secondary tier.
2. Minute: This field may contain either an asterisk ‘*’, which implies every minute or a numeric value between 0-59.
3. Hour: This field may contain either an asterisk ‘*’, which implies every hour, or a numeric value between 0-23.
4. Day of month: This field may contain either an asterisk ‘*’, which implies every day of the month, or a numeric value between 1-31.
5. Month: This field may contain either an asterisk ‘*’, which implies run every month, or a numeric value between 1-12. In addition to the numeric values, this field can also accept names of the month as an argument, with the first three letters of the month (all in lowercase) serving as input for the given parameter.
6. Day of Week: This field may contain either an asterisk ‘*’, which implies every day of the week, or a numeric value between 0-6, with 0 being interpreted as Sunday, 1 as Monday, and so on. In addition, this parameter can also accept names, with the first three letters of the month (all in lowercase) serving as input values.
7. Node Name: Cluster node name that executes the schedule. Default node name is the master node.

**Note:**

1. The parameters minute, hour, day-of-month, month, and day-of-week for tier schedule modify can accept numeric values in the form of ranges, where a range is defined as two numbers separated by a hyphen. So if you want to run the tiering schedule between 1 am and 4 am, then you can specify a value 1-4 for hour parameter, with the range being inclusive.
2. Similarly, you can specify a step value for other parameters, that is, day-of-month, month, and day-of-week as well. Step values are also allowed after an asterisk ‘*’, so if you want to run a schedule every two hours, you just have to specify ‘*/2’ as the input value for the ‘hour’ parameter.

So to move files from the primary to the secondary tier every two hours, use the following command:

```
tier schedule modify fs1 * */2 * * *
```

### 16.16.3 OPTIONS

- **size** Size of the tier of the file system (for example, 10m, 10M, 25g, 100G).
- **nmirrors** Number of mirrors.
**ncolumns**  Number of columns.

**protection=disk**  If the protection is set to disk, then mirrors are created on separate disks. The disks may or may not be in the same pool.

**protection=pool**  If the protection is set to pool, then mirrors are created in separate pools. If not enough space is available, then the file system creation operation fails.

**stripeunit=<kilobytes>**  Set the stripe width of the tier, where possible values of kilobytes are 128, 256, 512, 1024, and 2048.

```
tier add cloud fs_name tier_name service_name region
```

Add a cloud tier to the specified scale-out file system using service name and region. You can specify if you want to add an S3-compatible or Amazon Glacier cloud storage tier by specifying the appropriate option.

The supported regions of the Amazon S3 service are the following:

- California (us-west-1)
- Central (ca-central-1)
- Frankfurt (eu-central-1)
- Ireland (eu-west-1)
- London (eu-west-2)
- Mumbai (ap-south-1)
- Ohio (us-east-2)
- Oregon (us-west-2)
- Seoul (ap-northeast-2)
- Singapore (ap-southeast-1)
- Sydney (ap-southeast-2)
- Sao Paulo (sa-east-1)
- Tokyo (ap-northeast-1)
- Virginia (us-east-1)

The Amazon Glacier tier does not support the following regions: Singapore or Sao Paulo.

Region is irrelevant to an S3-compatible cloud storage service. If you select an S3-compatible service, select none as the region. Any other region specified with an S3-compatible service is ignored. Scale-out file system uses AWS signature version 4 to add authentication information to the requests sent to Amazon S3 and S3-compatible services. If an S3-compatible service cannot support AWS signature version 4, then it can not be added as a cloud tier to a scale-out file system. **Warning:** When a cloud storage service is used as a cloud tier for a scale-out file system, Veritas Access exclusively owns all the buckets and the objects created by Veritas Access. Any attempt to tamper with these buckets or objects outside of Veritas Access corrupts the files represented by those modified objects.

```
tier add simple fs_name size pool1 [, disk1,...]
```

Add a simple tier to the specified file system on one of the specified pools/disks.

```
tier add mirrored fs_name size nmirrors pool1 [, disk1,...] [protection=disk|pool]
```

Add a mirrored tier to the specified file system.

```
tier add striped fs_name size ncolumns pool1 [, disk1,...] [stripeunit=<kilobytes>]
```

Add a striped tier to the specified file system.
Add a mirrored-stripe tier to the specified file system.

tier add mirrored-stripe fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripe-unit=<kilobytes>]

Add a striped-mirror tier to the specified file system.

tier add striped-mirror fs_name size nmirrors ncolumns pool1 [, disk1,...] [protection=disk|pool] [stripe-unit=<kilobytes>]

Add a column to the tier file system.

tier addcolumn fs_name ncolumns pool1 [, disk1,...]

Remove a column from the tier file system.

tier rmcolumn fs_name

Remove a tier from the file system. All the files on the secondary tier get relocated to the primary tier. Ensure that you remove the policy by running the tier policy remove fs_name before running the tier remove command. When removing a cloud tier, the CLI expects that you specify the tier_name as well. If there is data present on the specified tier, then the tier remove operation fails, and the data is not automatically relocated.

tier list fs_name

Show the list of storage tiers configured on the specified scale-out file system. Display the tier type as S3 or Amazon Glacier.

tier move start fs_name source_tier destination_tier pattern {atime|mtime} {atime|mtime}

Start a job in the background that moves files that match the criteria from the source_tier to the destination_tier. Pattern identifies the files or directories to move. You can further restrict the files or directories to move by specifying the last accessed time (atime) or the last modified time (mtime). The atime and mtime criteria are optional. The move job returns a job ID for further tracking and control of the job. For the status of the job, use the tier move list command.

tier move dryrun fs_name source_tier destination_tier pattern {atime|mtime} {atime|mtime}

Start a job in the background that does not move the files, but performs a dry run (test) of the move operation. The move dryrun command calculates the number of files that match the criteria. To see the status of the job and to see the number of files calculated, use the tier move list command.

tier move list

List the background jobs for move and dry run. This command lists the job IDs and their status.

tier move status JOBID

This shows the detailed status of the job, which includes the job run type (dryrun or normal), state of the job, the total data to be moved, the total number of files to be moved, data moved so far, the number of files moved so far, and the last file visited.

tier move abort JOBID

Abort a job in its current state.

tier addmirror fs_name pool1 [, disk1,...] [protection=disk|pool]

Add a mirror to the tier of the file system.

tier rmmirror fs_name [pool_or_disk_name]

Remove a mirror from the tier of the file system that is spanning on the specified pools/disks.
tier listfiles \texttt{fs\_name} \{primary|secondary\}

Show all the files that are on the specified tier.

 tier mapfile \texttt{fs\_name file\_path}

Show the tier location of the specified file. The path of the file is relative to the file system. For example, \texttt{tier mapfile fsl /a.txt} shows the location of \texttt{a.txt}, which is in the root directory of the file system \texttt{fsl}.

 tier policy list

Show the policy for each tiered file system.

 tier policy prune list

Show the prune policy for each tiered file system.

 tier policy prune modify \texttt{fs\_name delete\_after}

Change the prune policy of the tiered file system. \texttt{delete\_after} specifies the number of days after which inactive files are deleted from the secondary tier.

 tier policy modify \texttt{fs\_name \{primary|secondary\} days minacctemp period}

Change the policy of the tiered file system. \texttt{(primary|secondary)} specifies the name of the tier on which the new files get created. \texttt{days} specifies the number of days after which inactive files are moved from the primary to the secondary tier. \texttt{period} is used for calculating the access temperature of a file. If the access temperature of a file exceeds more than \texttt{minacctemp}, then this file is moved from the secondary tier to the primary tier.

 tier relocate \texttt{fs\_name dirPath}

Relocate directory or file from the secondary tier to the primary tier. This does not relocate NDS (Named Data Stream also includes extended attributes) to the primary tier.

 tier policy remove \texttt{fs\_name}

Remove the policy of the tiered file system.

 tier policy prune remove \texttt{fs\_name}

Remove the prune policy of the tiered file system.

 tier policy run \texttt{fs\_name}

Run the policy of the tiered file system.

 tier schedule list

Show schedules of all the tiered file systems.

 tier schedule modify \texttt{fs\_name minute hour day\_of\_the\_month month year day\_of\_the\_week node\_name}

Modify the schedule of the tiered file system.

 tier schedule remove \texttt{fs\_name}

Remove the schedule of the tiered file system.

 tier query \texttt{fs\_name}

Show the list of files that are moved by running the policy.

 tier allowmetadata yes \texttt{fs\_name}
This allows the metadata information on the file system to be written on the secondary tier as well. By default, the secondary tier is not configured for storing the metadata information of the file system. Tiers configured with this option show `metaOK` in the column `SECONDARY TIER` of the `fs list` output.

```bash
tier allowmetadata no fs_name
```
This restricts the metadata information to the primary tier only. If the primary tier gets full, the writes to the secondary tier are not served, as the metadata updates are restricted to the primary tier only.

```bash
tier setfastresync fs_name pool1 [, disk1,...]
```
Set fastresync for the tiers of the file system.

```bash
tier unsetfastresync fs_name
```
Unset fastresync for the tiers of the file system.

```bash
tier stats {show|reset|usage} fs_name tier_name
```
Show the access statistics, reset the access statistics to zero, or show the total usage of the specified cloud tier in the `largefs` file system.

```bash
tier stats monitor fs_name tier_name [interval]
```
Monitor the access statistics of the specified cloud tier in the `largefs` file system. The default interval is five seconds.

### 16.16.4 EXAMPLES

Create a mirrored file system with name `fs1` with disks from the pools `pool1` and `pool2`. Add a mirrored tier to this file system.

```bash
Storage> fs create mirrored fs1 100M 2 pool1,pool2
100% [#] Creating mirrored filesystem
Storage> tier add mirrored fs1 100M 2 pool3,pool4
100% [#] Creating mirrored secondary tier of filesystem
```

Add a mirror to the secondary tier of the file system `fs1`.

```bash
Storage> tier addmirror fs1 pool5
100% [#] Adding mirror to secondary tier of filesystem
```

Add a column to the tier file system.

```bash
Storage> tier addcolumn fs1 1 pool1
ACCESS fs INFO V-288-2644 This operation may take some time to complete. You can→ check the status in storage fs list fsname
```

Remove a column from the tier file system.

```bash
Storage> tier rmcolumn fs1
ACCESS fs INFO V-288-2711 Only one column will be removed.
ACCESS fs INFO V-288-2644 This operation may take some time to complete. You can→ check the status in storage fs list fsname
```

Show the list of files on the primary tier of file system `fs1`.

```bash
Storage> tier listfiles fs1 primary
/.placement_policy.xml
/lost+found/changelog
```
Show the list of files on the secondary tier of file system fs1.

```
Storage> tier listfiles fs1 secondary
```

Show tier location of file a.txt, which is in the root directory of file system fs1.

```
Storage> tier mapfile fs1 /a.txt
Tier Extent Type File Offset Extent Size
==== =========== =========== ===========
Primary Data 0 Bytes 1.00 KB
```

The following command sets the policy of file system fs1 such that the new files get created on the primary tier. If a file has not been accessed for more than 7 days, then it is moved from the primary to the secondary tier, and if the access temperature of files in the secondary tier is more than 5, then these files are moved from the secondary tier to the primary tier. Access temperature is calculated over a 3-day period.

```
Storage> tier policy modify fs1 primary 7 5 3
ACCESS fs SUCCESS V-288-0 Successfully modified tiering policy for file system `fs1`
```

List the tiering policy for all the file systems.

```
Storage> tier policy list
FS Create on Days MinAccess Temp PERIOD
========================== ========= ==== ============== ======
fs1 primary 7 5 3
```

Modify the prune policy.

```
Storage> tier policy prune modify fs1 180
ACCESS fs SUCCESS V-288-0 Successfully modified the prune policy for file system fs1
```

List the tiering prune policy for all the file systems.

```
Storage> tier policy prune modify fs1 180
FS Delete After
========================= =========
fs1 180
```

Run the tiering policy for file system fs1.

```
Storage> tier policy run fs1
ACCESS fs SUCCESS V-288-0 Successfully ran tiering policy for File system fs1
```

Show the list of files that are moved and or deleted by running the policy.

```
Storage> tier query fs1
/a.txt
/b.txt
/c.txt
/d.txt
```

Set the schedule of file system fs1. Default node name is the master node.

```
Storage> tier schedule modify fs1 1 1 1 * *
ACCESS fs SUCCESS V-288-0 Command 'tier schedule modify' executed successfully for fs1
```

Get the tiering schedule for all the file systems.
Storage> tier schedule list

<table>
<thead>
<tr>
<th>FS</th>
<th>Minute</th>
<th>Hour</th>
<th>Day</th>
<th>Month</th>
<th>WeekDay</th>
<th>NodeName</th>
</tr>
</thead>
<tbody>
<tr>
<td>fs1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>*</td>
<td>*</td>
<td>master node</td>
</tr>
</tbody>
</table>

Remove the tiering schedule for file system fs1.

Storage> tier schedule remove fs1
ACCESS fs SUCCESS V-288-0 Command tier schedule remove executed successfully for fs1

Remove the policy of file system fs1.

Storage> tier policy remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed tiering policy for File system fs1

Remove the prune policy of file system fs1.

Storage> tier policy prune remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed the Prune policy for File system fs1

Remove a mirror from the secondary tier of file system fs1.

Storage> tier rmmirror fs1

Remove the cloudtier from file system fs1.

Storage> tier remove fs1 cloudtier

Allow storing metadata information to the secondary tier.

Storage> tier allowmetadata yes fs1
ACCESS fs SUCCESS V-288-0 Configured the secondary tier for storing metadata information.

Restrict storing metadata information to the primary tier.

Storage> tier allowmetadata no fs1
ACCESS fs SUCCESS V-288-0 Configured the secondary tier for storing no metadata information.

Set fastresync for the tiers of the file system.

Storage> tier setfastresync adistr pool1

Unset fastresync for the tiers of the file system.

Storage> tier unsetfastresync adistr
ACCESS fs SUCCESS V-288-1817 Disabled fast resync on the file system adistr

Add the cloud storage of the Amazon S3 service, named awstest, in the region of us-west-2 as the cloud tier cloudtier for the scale-out file system largefs1.

Storage> tier add cloud largefs1 cloudtier awstest us-west-2
ACCESS tier SUCCESS V-288-0 Tier cloudtier is added for largefs1

Add S3-compatible cloud storage, named s3comptest, as the cloud tier for the scale-out file system largefs1. Use none as the region for S3-compatible cloud storage.
Add an Amazon Glacier cloud storage tier.

```
Storage> tier add cloud gfs2 gtier2 gserv California Glacier
ACCESS tier SUCCESS V-288-0 Tier gtier2 is added for gfs2
```

Show the list of storage tiers for the scale-out file system largefs1.

```
Storage> tier list largefs1
TIER NAME TIER TYPE PROVIDER SERVICE NAME
========== ========= ========= =============
primary DISK      ------- -------
cloudtier CLOUD AWS     amazon_service
```

Remove the cloud tier cloudtier from the scale-out file system largefs1.

```
Storage> tier remove largefs1 cloudtier
ACCESS tier SUCCESS V-288-0 Tier cloudtier is removed
```

Move the files with the name pattern *.txt, that have not been accessed within the past 100 days from the disk tier primary to the cloud tier cloudtier.

```
Storage> tier move start largefs1 primary cloudtier */*.txt atime >100D
ACCESS Tier SUCCESS V-288-0 The job has been started. ID is 1473682883.
```

Specify the retrieval options for retrieving data from Amazon Glacier. Expedited retrievals typically complete within 1-5 minutes. Standard retrievals typically complete within 3-5 hours. Bulk retrievals typically complete within 5-12 hours. The Bulk option is the default. An EIO error is returned for read, write, or truncate until the files are moved to the primary tier (which could be 1-5 minutes, or 3-5 hours, or 5-12 hours).
Move all the files to the tier primary.

Perform a dry run of the tier move operation. A dry run can be used for estimating the scope of the tier movement of files.

List all the tier move jobs.

Show the status of a tier move job.

Show the access statistics of the cloud tier cloudtier.

Monitor the access statistics of the cloud tier cloudtier every 10 seconds.

Reset the access statistics of the cloud tier cloudtier to zero. After executing the tier stats reset command, the output for the tier stats show command is reset to zero.

Show the usage of the cloud tier cloudtier.
Veritas Access Command Reference Guide Documentation, Release 7.3

```
Storage> tier stats usage largefs1 cloudtier
Storage Utilized       223.1GB
Number of objects     488
Number of files       231
```

16.16.5 SEE ALSO

disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), iscsi(1), quota(1)
16.17  **uncompress**

16.17.1  **SYNOPSIS**

    uncompress file fs_name f{file|dir} res_level

16.17.2  **DESCRIPTION**

    uncompress file fs_name f{file|dir} res_level  Uncompress a file on the fs_name file system.

16.17.3  **EXAMPLES**

Uncompress file data1.dbf in file system tpcc_arch1 using high resource level.

    Storage> uncompress file tpcc_arch1 data1.dbf high
    ACCESS uncompression Success V-288-999 Uncompression completed

16.17.4  **SEE ALSO**

    disk(1), hba(1), fencing(1), fs(1), pool(1), scanbus(1), snapshot(1), tier(1), iscsi(1), cifs(1)
17.1 support

17.1.1 SYNOPSIS

debuginfo setlog loglevel
debuginfo upload nodename debug-URL module
iostat cpu [nodename] [interval] [count]
iostat device [nodename] [dataunit] [interval] [count]
tethereal export url [nodename] [interface] [count] [source]
tethereal show [nodename] [interface] [count] [source]
top [nodename] [iterations] [delay]
traceroute destination [source] [maxttl]
metasave [fsname] [output_location]
services autofix
services online servicename
services show
services showall

17.1.2 DESCRIPTION

These support utility commands are used to debug any problems that occur within the cluster.

17.1.3 OPTIONS

   debuginfo setlog loglevel  This command set CIFS log level in the cluster.
debuginfo upload nodename debug-URL module This command uploads debug information of given module from specified node to the external server. The debug-URL can be a remote file or directory. If debug-URL specifies a remote file, the debuginfo file will be saved by that name; if debug-URL specifies a remote directory, the debuginfo file will have the name like nas_debuginfo_nodename_modulename_timestamp.tar.gz. Supported module values are [all|generic|cif|shnas|supportconfig].

iostat cpu [nodename] [interval] [count] This command generates CPU and IO statistics information. When the iostat cpu command is executed for the first time it contains information since the system was booted. Each subsequent CPU utilization report shows the details since the last report. nodename contains the name of the node from where report is generated. By default it accepts ‘console’ as the Management Console. Interval and count specify the amount of time in seconds between each report and number of reports, respectively.

iostat device [nodename] [dataunit] [interval] [count] This command generates the device utilization report. When the iostat device command is executed for the first time it contains information since the system was booted. Each subsequent device utilization report shows the details since the last report. It has two optional parameters. The first parameter, nodename, contains the name of the node that the report is generated from. By default it accepts ‘console’ as the Management Console. The second parameter is the report that can be generated in block(s) or kilobyte(s). By default all of the data is in block(s). Interval and count specify the amount of time in seconds between each report and number of reports, respectively.

tethereal export url [nodename] [interface] [count] [source] This command exports the network traffic details. The url provides the location to export the network traffic details. The default file name is tethereal.log, if it is not specified in url. The nodename contains the name of the node from where traffic details are generated. By default it accepts ‘console’ as the Management Console. The interface specifies the network interface for packet capture. The count specifies the maximum number of packets to read. A packet can be filtered by specifying the source node.

tethereal show [nodename] [interface] [count] [source] This command displays the network traffic details for a given nodename. By default it accepts ‘console’ as the Management Console. The interface specifies the network interface for the packet capture. The count specifies the maximum number of packets to read. A packet can be filtered by specifying the source node.

top [nodename] [iterations] [delay] This command provides the dynamic look of processor activity in real time and displays the list of CPU intensive tasks. It shows resources consumed by users and processes at a given time for a given nodename. The iterations parameter specifies the number of iterations (the default is 3). The delay parameter specifies the delay between screen updates (the default is 5 seconds).

traceroute destination [source] [maxttl] This command shows the route between two nodes by orderly listing all of the intermediate nodes over the network. It displays how a node is connected to the internet and eventually to a specified target destination; or in between the gateway that is discarding packets. The source and maxttl specify the source node name to begin the trace and the maximum number of hops (the default is 7).

metasave [fsname] [output_location] Collects Metasave image of a regular or a largefs File System specified by fsname. The Metasave image is stored at the directory location specified by output_location. For regular File System a single Metasave image will be created under output_location. For a largefs File System multiple Metasave images will be produced depending on number of container File Systems inside the largefs File System. For largefs File System the namespace mapping database is also dumped.

services autofix Attempts to fix any faults with any services on all of the running nodes in the cluster.

services online servicename Brings a service online. If servicename is a parallel service that can
be brought online on all nodes, an attempt is made to bring the service online on all of the nodes. If _servicename_ is a failover service, an attempt is made to bring the service online on any of the running nodes in the cluster. If the _servicename_ is already online, no action is taken.

`servicename` Displays the state of the services on all the running nodes in the cluster. State of the IPs and file systems are shown only if they are not online. It might also attempt to fix any faults with any services.

`services show` Displays the state of all of the services on all the running nodes in the cluster. It might also attempt to fix any faults with any of the services.

### 17.1.4 EXAMPLES

Set CIFS loglevel to 10 in the cluster.

Support> debuginfo setlog 10

Upload all debug information to an FTP server.

Support> debuginfo upload node1_1
ftp://admin@ftp.docserver.veritas.com/patches/ all

Upload CIFS related debug information to an SCP server.

Support> debuginfo upload node1_1
scp://root@server.veritas.com:/tmp/ cifs

Shows the cpu statistics.

Support> iostat cpu test_01 1 1
Linux 2.6.16.60-0.21-smp (test_01) Wednesday 08 July 2009

avg-cpu: %user %nice %sys %iowait %idle
 0.14 0.01 0.12 0.01 99.72

Shows the device statistics.

Support> iostat device test_01 Blk 1 1
Linux 2.6.16.60-0.21-smp (test_01) Wednesday 08 July 2009

Device:      tps Blk_read/s Blk_wrtn/s Blk_read Blk_wrtn
sda          2.91   6.54   63.73   628792   6123480
sdb          0.00   0.01   0.00    904        0
sdc          0.00   0.03   0.00   2514        0
sdd          0.02   0.69   0.06   66034      5409
sde          0.01   0.62   0.59   59929      56314
sdf          0.00   0.03   0.00   2514        0

Show the network traffic.

Support> tethereal show test_01 pubeth0 5 172.31.168.140
0.000000 172.31.168.140 -> 10.209.105.147 ICMP Echo (ping) request
0.000276 10.209.105.147 -> 172.31.168.140 ICMP Echo (ping) reply
0.000473 10.209.105.147 -> 172.31.168.140 SSH Encrypted response packet len=112
0.000492 10.209.105.147 -> 172.31.168.140 SSH Encrypted response packet len=112
0.000845 172.31.168.140 -> 10.209.105.147 TCP 50777 > 22 [ACK] Seq=0 Ack=112...
  Win=3624 Len=0
Export the network traffic.

Support> tethereal export scp://user1@172.31.168.140:~/
Password: ******
Capturing on pubeth0 ...
Uploading network traffic details to scp://user1@172.31.168.140:~/ is completed.

Display the dynamic real-time view of the tasks.

Support> top test_01 1 1
top - 16:28:27 up 1 day, 3:32, 4 users, load average: 1.00, 1.00, 1.00
Tasks: 336 total, 1 running, 335 sleeping, 0 stopped, 0 zombie
Cpu(s): 0.1% us, 0.1% sy, 0.0% ni, 99.7% id, 0.0% wa, 0.0% hi, 0.0% si
Mem: 16405964k total, 1110288k used, 15295676k free, 183908k buffers
Swap: 1052248k total, 0k used, 1052248k free, 344468k cached

PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
6314 root 15 0 5340 1296 792 R 3.9 0.0 0:00.02 top
1 root 16 0 640 260 216 S 0.0 0.0 0:04.86 init

Trace the route to network host.

Support> traceroute www.veritas.com test_01 10
traceroute to www.veritas.com (8.14.104.56), 10 hops max, 40 byte packets
1 10.209.104.2 0.337 ms 0.263 ms 0.252 ms
2 10.209.186.14 0.370 ms 0.340 ms 0.326 ms
3 puna-spi-core-b02-vlan105hsrp.net.veritas.com (143.127.185.130) 0.713 ms 0.525 ms 0.533 ms
4 143.127.185.197 0.712 ms 0.550 ms 0.564 ms
5 10.212.252.50 0.696 ms 0.600 ms 78.719 ms

Display the state of important services.

Support> services show
Verifying cluster state...........done

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfss</td>
<td>ONLINE</td>
<td>STARTING</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>FAULTED</td>
<td>FAULTED</td>
</tr>
</tbody>
</table>

Display the state of all of the services.

Support> services showall

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfss</td>
<td>ONLINE</td>
<td>STARTING</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
</tbody>
</table>
Bring a service online.

Support> services online 10.216.50.132
Support> services show

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfs</td>
<td>ONLINE</td>
<td>STARTING</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>OFFLINE</td>
<td>STARTING</td>
</tr>
</tbody>
</table>

Autofix all the services.

Support> services autofix
Attempting to fix service faults........done
Support> services show

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>nfs</td>
<td>ONLINE</td>
<td>STARTING</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>FAULTED</td>
<td>FAULTED</td>
</tr>
<tr>
<td>Service</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td>nfs</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
<td></td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>OFFLINE</td>
<td></td>
</tr>
</tbody>
</table>
17.2 debuginfo

17.2.1 SYNOPSIS

d debuginfo setlog cifs loglevel
d debuginfo setlog nbu database loglevel
d debuginfo setlog nbu global loglevel
d debuginfo setlog nbu enable critical
d debuginfo setlog nbu enable robust
d debuginfo upload nodename debug-URL module

17.2.2 DESCRIPTION

The debuginfo commands can set the CIFS or the NBU client log levels in the cluster, as well as upload debug information to an external FTP or SCP server.

17.2.3 OPTIONS

 debuginfo setlog cifs loglevel Set CIFS log level in the cluster. Valid log level value ranges from 0 to 10, 10 being the most detailed. Default is 2.

d debuginfo setlog nbu database loglevel Set NetBackup database debugging log level in the cluster. Valid log level value ranges from 1 to 5, 5 being the most detailed.

d debuginfo setlog nbu global loglevel Set the NetBackup global debugging log level in the cluster. Valid log level value ranges from 1 to 5, 5 being the most detailed.

d debuginfo setlog nbu enable robust Enable the NetBackup client to perform robust logging in the cluster.

d debuginfo setlog nbu enable critical Enable the NetBackup client to perform critical process logging in the cluster.

d debuginfo upload nodename debug-URL module Upload debugging information of given module from specified node to the external server. The debug-URL can be a remote file or directory. If debug-URL specifies a remote file, the debuginfo file will be saved by that name; if debug-URL specifies a remote directory, the debuginfo file uses a name like nas_debuginfo_nodename_modulename_timestamp.tar.gz. Supported module values are [all|generic|cifs|nas|netbackup|supportconfig]. Use all to collect all information needed for debug, generic to collect all information except Veritas product information, cifs to collect CIFS related information, nas to collect product-related information, netbackup to collect NetBackup-related information, supportconfig to collect system support-related information.

17.2.4 EXAMPLES

Set CIFS log level to 10 in the cluster.

Support> debuginfo setlog cifs 10
Upload all debug information to an FTP server.

```
Support> debuginfo upload node1_1
ftp://admin@ftp.docserver.veritas.com/patches/ all
```

Upload CIFS related debug information to an SCP server.

```
Support> debuginfo upload node1_1
scp://root@server.veritas.com:/tmp/ cifs
```

Upload CIFS related debug information to file in debug_dir directory on a node.

```
Support> debuginfo upload node1_1
file:///debug_dir/ cifs
```

Set NetBackup client database log level to 3 in the cluster.

```
Support> debuginfo setlog nbu database 3
```
17.3 iostat

17.3.1 SYNOPSIS

iostat cpu [nodename] [interval] [count]
iostat device [nodename] [dataunit] [interval] [count]

17.3.2 DESCRIPTION

iostat commands display the CPU and I/O statistics.

17.3.3 OPTIONS

iostat cpu [nodename] [interval] [count] This command generates CPU and I/O statistics. When the iostat cpu command is executed for the first time, the output contains information from when the system was booted. Each subsequent CPU utilization report displays the details since the last report. The nodename contains the name of the node that the report is generated from. By default, it uses the term ‘console’ for the Management Console. Interval and count specify the amount of time in seconds between each report and number of reports, respectively.

iostat device [nodename] [dataunit] [interval] [count] This command generates the utilization report of the device. When the iostat device command is executed for the first time, it contains information from when the system was booted. Each subsequent device utilization report shows the details since the last report. It has two optional arguments. The first argument, *nodename*, contains the name of the node that the report is generated from. By default, it uses the term ‘console’ for the Management Console. The report can be generated in terms of block(s) or kilobyte(s) by specifying the second argument. Unless specified, all of the data will be in block(s). Interval and count specify the amount of time in seconds between each report and number of reports, respectively.

17.3.4 EXAMPLES

Shows the cpu statistics.

Support> iostat cpu test_01 1 1
Linux 2.6.16.60-0.21-smp (test_01) Wednesday 08 July 2009

    avg-cpu: %user %nice %sys %iowait %idle
         0.14  0.01  0.12  0.01  99.72

Shows the device statistics.

Support> iostat device test_01 Blk 1 1
Linux 2.6.16.60-0.21-smp (test_01) Wednesday 08 July 2009

    Device:     tps  Blk_read/s  Blk_wrtn/s  Blk_read  Blk_wrtn
    sda  2.91  6.54  63.73 628792 6123480
    sdb  0.00  0.01  0.00   904     0
    sdc  0.00  0.03  0.00  2514     0
    sdd  0.02  0.69  0.06  66034  5409
    sde  0.01  0.62  0.59  59929  56314
    sdf  0.00  0.03  0.00  2514     0
17.3.5 SEE ALSO

tethereal(1), top(1), traceroute(1)
17.4 metasave

17.4.1 SYNOPSIS

metasave [fsname] [output_location]

17.4.2 DESCRIPTION

metasave command collects metasave image of a regular or scale-out file system for debugging purposes.

17.4.3 OPTIONS

metasave [fsname] [output_location] Collects Metasave image of a regular or a scale-out file system specified by fsname. The Metasave image is stored at the directory location specified by output_location. For a CFS file system, a single Metasave image is created under output_location. For a scale-out file system, multiple Metasave images are produced depending on the number of container file systems inside the scale-out file system. For the scale-out file system, the namespace mapping database is also dumped.

17.4.4 EXAMPLES

Collect metasave of file system testfs and store it under /tmp/meta_out_dir.

Support> metasave testfs /tmp/meta_out_dir
Collecting Metasave image of File System testfs. This may take some time...
SUCCESS: Metasave image of testfs collected succesfully. TAR Image is stored at /tmp/...meta_out_dir/metastave_tempfs.tar.

17.4.5 NOTE

File system must be offline on all the cluster nodes to create a consistent metasave image. Bring the file system offline before collecting metasave using the Storage>fs offline command. Metasave image collection is a time-consuming operation. Total time taken depends on the amount of metadata information present in the file system. Time taken for scale-out file system can be significantly higher. Other Veritas Access operations can be run from a separate terminal while the metasave collection is in progress.

17.4.6 SEE ALSO

iostat(1), debuginfo(1), fs(1)
17.5 services

17.5.1 SYNOPSIS

services autofix
services online servicename
services show
services showall

17.5.2 OPTIONS

servicename   Name of the service that needs to be online.

services autofix   Attempts to fix any faults with any services on all of the running nodes of the
                   cluster.

services online servicename   Brings a service online. If servicename is a parallel service that
                               can be onlined on all nodes, an attempt is made to bring the service online on all of the
                               nodes. If servicename is a failover service, an attempt is made to bring the service online
                               on any of the running nodes in the cluster. If servicename is already online, no action is
                               taken.

services show   Shows the state of the services on all of the running nodes of the cluster. The state of
                 the IPs and file systems are shown only if they are not online. It might also attempt to fix
                 any faults with any of the services.

services showall   Shows the state of all the services on all of the running nodes of the cluster. It
                    might also attempt to fix any faults with any of the services.

17.5.3 EXAMPLES

Display the state of important services.

```
Support> services show
Verifying cluster state..........done

<table>
<thead>
<tr>
<th>Service</th>
<th>test</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
</tr>
<tr>
<td>nfs</td>
<td>ONLINE</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>FAULTED</td>
</tr>
</tbody>
</table>
```

Display the state of all of the services.

```
Support> services showall
```
### Bring a service online.

```bash
Support> services online 10.216.50.132
Support> services show
```

### Autofix all of the services.

```bash
Support> services show
```

---

```bash
Support> services autofix
Attempting to fix service faults............done
```

### 17.5. services
Support> services show

<table>
<thead>
<tr>
<th>Service</th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nfs</td>
<td>ONLINE</td>
<td>STARTING</td>
</tr>
<tr>
<td>cifs</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>ftp</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>http</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>backup</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>console</td>
<td>ONLINE</td>
<td>OFFLINE</td>
</tr>
<tr>
<td>nic_pubeth0</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>nic_pubeth1</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>fs_manager</td>
<td>ONLINE</td>
<td>ONLINE</td>
</tr>
<tr>
<td>10.216.50.132</td>
<td>OFFLINE</td>
<td>STARTING</td>
</tr>
</tbody>
</table>
17.6 tethereal

17.6.1 SYNOPSIS

\texttt{tethereal export url [nodename] [interface] [count] [source]}
\texttt{tethereal show [nodename] [interface] [count] [source]}

17.6.2 DESCRIPTION

\texttt{tethereal} commands dump and analyze the network traffic.

17.6.3 OPTIONS

\texttt{tethereal export url [nodename] [interface] [count] [source]} This command exports the network traffic details. \texttt{url} provides the location to export the network traffic details. Default file name is \texttt{tethereal.log}, if it is not specified in \texttt{url}. \texttt{nodename} contains the name of the node from where traffic details are generated; by default, it takes ‘console’ for the Management Console. \texttt{interface} and \texttt{count} specify the network interface for packet capture and maximum number of packets to read, respectively. Packet can be filtered by specifying \texttt{source} node. Press the \texttt{Ctrl+C} to stop the capture process and upload traffic details to the \texttt{url} site.

\texttt{tethereal show [nodename] [interface] [count] [source]} This command displays the network traffic details for a given \texttt{nodename}; by default, it takes ‘console’ for the Management Console. \texttt{interface} and \texttt{count} specify the network interface for packet capture and maximum number of packets to read, respectively. Packet can be filtered by specifying \texttt{source} node.

17.6.4 EXAMPLES

Show the network traffic.

\begin{verbatim}
Support> tethereal show test_01 pubeth0 5 172.31.168.140
 0.000000 172.31.168.140 -> 10.209.105.147 ICMP Echo (ping) request
 0.000276 10.209.105.147 -> 172.31.168.140 ICMP Echo (ping) reply
 0.000473 10.209.105.147 -> 172.31.168.140 SSH Encrypted response packet len=112
 0.000492 10.209.105.147 -> 172.31.168.140 SSH Encrypted response packet len=112
 0.000845 172.31.168.140 -> 10.209.105.147 TCP 50777 > 22 [ACK] Seq=0 Ack=112 ...
\end{verbatim}

Export the network traffic.

\begin{verbatim}
Support> tethereal export scp://user1@172.31.168.140:~/
Password: ******
Capturing on pubeth0 ...
Uploading network traffic details to scp://user1@172.31.168.140:~/ is completed.
\end{verbatim}

17.6.5 SEE ALSO

\texttt{iostat(1), top(1), traceroute(1)}

\addcontentsline{toc}{section}{17.6. tethereal}
17.7 top

17.7.1 SYNOPSIS

top [nodename] [iterations] [delay]

17.7.2 DESCRIPTION

top command provides dynamic look of processor activity in real-time.

17.7.3 OPTIONS

    top [nodename] [iterations] [delay]  The top command provides a dynamic look of processor activity in real-time and displays the list of CPU intensive tasks. It shows resources consumed by users and processes at a given time for a given nodename. iterations and delay specify the number of iterations (by default 3) and delay between screen updates (by default 5 seconds), respectively.

17.7.4 EXAMPLES

Display the dynamic real-time view of a task.

Support> top test_01 1 1
    top - 16:28:27 up 1 day, 3:32, 4 users, load average: 1.00, 1.00, 1.00
    Tasks: 336 total, 1 running, 335 sleeping, 0 stopped, 0 zombie
    Cpu(s): 0.1% us, 0.1% sy, 0.0% ni, 99.7% id, 0.0% wa, 0.0% hi, 0.0% si
    Mem: 16405964k total, 1110288k used, 15295676k free, 183908k buffers
    Swap: 1052248k total, 0k used, 1052248k free, 344468k cached

    PID USER PR NI VIRT RES SHR S %CPU %MEM TIME+ COMMAND
    6314 root 15 0 5340 1296 792 R 3.9 0.0 0:00.02 top
    1 root 16 0 640 260 216 S 0.0 0.0 0:04.86 init

17.7.5 SEE ALSO

iostat(1), thereal(1), traceroute(1)
17.8 traceroute

17.8.1 SYNOPSIS

traceroute destination [source] [maxttl]

17.8.2 DESCRIPTION

traceroute command shows the route from a node to a specified target.

17.8.3 OPTIONS

traceroute destination [source] [maxttl] traceroute shows the route between two nodes by orderly listing all the intermediate nodes over the network. It displays how a node is connected to the Internet and eventually to a specified target destination; or an in-between gateway that is discarding packets. source and maxttl specify the source node name to begin trace and maximum number of hops (by default 7).

17.8.4 EXAMPLES

Trace the route to the network host.

Support> traceroute www.veritas.com test_01 10
traceroute to www.veritas.com (8.14.104.56), 10 hops max, 40 byte packets
1 10.209.104.2 0.337 ms 0.263 ms 0.252 ms
2 10.209.186.14 0.370 ms 0.340 ms 0.326 ms
3 puna-spi-core-b02-vlan105hsrp.net.veritas.com (143.127.185.130) 0.713 ms 0.525 ms
4 143.127.185.197 0.712 ms 0.550 ms 0.564 ms
5 10.212.252.50 0.696 ms 0.600 ms 78.719 ms

17.8.5 SEE ALSO

iostat(1), tethereal(1), top(1)
18.1 system

18.1.1 SYNOPSIS

clock show
clock set time day month year
clock timezone timezone
clock regions [region]
config export local file_name
config export remote URL
config import local file_name

{ network|admin|all|report|system|cluster_specific|all_except_cluster_specific
  nfs|cifs|ftp|backup|replication|storage_schedules|storage_quota|storage_fs_alert|
  compress_schedules|defrag_schedules|storage_dedup|smartio }

config import remote URL

{ network|admin|all|report|system|cluster_specific|all_except_cluster_specific
  nfs|cifs|ftp|backup|replication|storage_schedules|storage_quota|storage_fs_alert|
  compress_schedules|defrag_schedules|storage_dedup|smartio }

config delete file_name
config list
guientable
guidisable
guistatus
kms config list
kms config status
kms config server server_ip server_port
kms config delete
kms certificate generate
kms certificate import_server_cert
kms certificate import_client_key
kms certificate import_client_cert
license add <path_of_key_file>
license list
license list details
more enable
more disable
more status
ntp servername server-name
ntp show
ntp enable
ntp disable
ntp sync
option show nfsd
option show cfsmount_ontimeout
option show dmpio
option show ninodes
option show tunerstab fs-name
option show tunefstab
option modify nfsd number [nodename]
option modify dmpio {enclosure enclr_name | arrayname
array_name | arraytype A/A/A/P... }
iopolicy={adaptive | adaptiveminq | balanced
minimumq | priority | round-robin | singleactive}
[nodename={nodename||}]
option modify ninodes { number | Auto }
option modify tunerstab initial_extent_size value fs-name
option modify tunerstab read_nstream value fs-name
option modify tunerstab read_pref_io value fs-name
option modify tunerstab write_nstream value fs-name
option modify tunerstab write_pref_io value fs-name
option modify tunerstab write_throttle value fs-name
option modify dmptune dmp_path_age value
option modify dmptune dmp_health_time value
stat sys [node]
stat cluster
stat dmp [node]
stat fsio [fsname]
stat all [node]
stat rdma [node]
webservices server [start|stop|status]
webservices SSL certificate certificate_path
webservices SSL disable
webservices SSL enable
webservices user password

18.1.2 DESCRIPTION
The system commands set or show the date and time of the system, and start, stop, sync or check the status of the NTP server. It also contains commands related to showing cluster-wide performance statistics and commands. An administrator can enable or disable the more filter on output of the admin console with the help of the more command present in this category. It also contains the option command display for configuring the tunable parameters. It also contains the license commands which provide options to perform necessary operations related to licensing. It also contains the kms commands that register or unregister the cluster with the KMS server.

18.1.3 OPTIONS

clock show  Display the current time and date of the system.

clock set time day month year  Set the current date and time of the system. The format of time, day, month, and year is given below:

*time*: HH:MM:SS using a 24 hour clock
*day*: 1..31
*month*: January | February | March | April | May | June | July | August | September | October | November | December
*year*: YYYY

clock timezone timezone  Set the timezone to the specified name of the time zone.

clock regions [region]  Display the list of regions. Regions can be one of the following:

{$Africa, America, Asia, Australia, Canada, Europe, GMT-offset, Pacific, US$}

cfg export local file_name  Save the configuration in a local file.

cfg export remote URL  Save the configuration on a remote machine. Exported File is named export.tar.gz if no file name is specified in the URL. Note: When exporting files with ftp URL, the given path is considered relative to the current working directory of the session. For example, to get the file named README from your home directory on your ftp site, use:
But if you want to get the README file from the root directory of the site, you need to specify the absolute file name:

```
ftp://user:passwd@my.site.com//README
```

(that is, with an extra slash in front of the file name.)

**config import local file_name**

```
{ network|admin|all|report|system|cluster_specific|all_except_cluster_specific|nfs|cifs|ftp|backup|replication|storage_schedules|compress_schedules|defrag_schedules|storage_dedup|smartio}
```

Import the specified configuration saved in a local file. **Note** For importing cifs local users/groups you have to import admin module also.

**config import remote URL**

```
{ network|admin|all|report|system|cluster_specific|all_except_cluster_specific|nfs|cifs|ftp|backup|replication|storage_schedules|compress_schedules|defrag_schedules|storage_dedup|smartio}
```

Import the specified configuration from a remote machine. **Note** For importing cifs local users/groups you have to import admin module also. **Note**: When exporting files with ftp URL, the given path is considered relative to the current working directory of the session. For example, to get the file named README from your home directory on your ftp site, use:

```
ftp://user:passwd@my.site.com/README
```

But if you want to get the README file from the root directory of the site, you need to specify the absolute file name:

```
ftp://user:passwd@my.site.com//README
```

(i.e. with an extra slash in front of the file name.)

**config delete file_name** Delete the locally saved configuration file.

**config list** View the list of locally saved configuration files.

**guienable** The system guienable command enables use of the GUI Management Server.

**guidisableable** The system guidisable command disables use of the GUI Management Server.

**guistatus** The system guistatus displays status of the GUI Management Server.

**kms config list** Display the registered KMS server details.

**kms config status** List the status of SSL certificate files that are configured on the cluster.

**kms config server server_ip server_port** Register the KMS server with cluster.

**kms config delete** Delete the KMS server details.

**kms certificate generate** Generate SSL self-signed keypair on cluster. It is advised that cluster nodes’ time settings are synchronized with NTP server before generating self-signed certificates.

**kms certificate import_server_cert** Import the KMS servers public key.

**kms certificate import_client_key** Import the SSL key file of the cluster that is used in CSR.

**kms certificate import_client_cert** Import the CA signed public key of the cluster.
license add <path_of_key_file> Adds or installs the license using the .slf key file which is provided. The scp protocol is also supported for adding license. The scp path should be specified: scp://user@ip:<path_of_key_file>

license list Lists the type of license installed on the cluster. The license type can be trialware (trial license for 60 days), subscription (license with validity of 1 year) or perpetual (permanent license).

license list details Lists the details of the license installed on the cluster such as the product name, version, start date, end date, license type, current state etc.

more enable Enable the more filter with the output of the admin console command.

more disable Disable the more filter with the output of the admin console command.

more status Display the status of the more filter.

ntp show Display the NTP status and server name.

ntp enable Enable NTP on all the nodes in the cluster.

ntp disable Disable NTP on all the nodes in the cluster.

ntp servername server-name Set the NTP server on all the nodes in the cluster. Use 127.127.1.0 as the server name to set the local clock.

ntp sync Snc date with NTP server on all the nodes in the cluster. Note NTP should be disabled before running “ntp sync” command.

option show nfsd Display the number of nfs daemons for each node in a cluster.

option show cfsmount_ontimeout Display cfsmount online timeout.

option show dmpio Display the type of iopolicy corresponding to enclosure, arrayname, arraytype for each node.

option show ninodes Display the global inode cache size.

option show tunefstab fs-name Display the file-system specific tunefstab parameters and their value for the specified file system.

option show dmptune Display the value of the dmptune attribute.

option modify nfsd number [nodename] Modify the number of daemons. The range for the number of daemons is from 1 to 512.

option modify cfsmount_ontimeout Value Modify cfsmount online timeout. The range is from 300 to 9000. The default timeout value is 1200 seconds.

option modify dmpio {enclosure enclr_name | arrayname

array_name | arraytype {A/A|A/P|...}} iopolicy={adaptive | adaptiveminq | balanced minimumq | priority | round-robin | singleactive} [nodename={nodename|‘‘}]

Modify the dmpio policy corresponding to enclosure, arrayname, arraytype.

option modify ninodes { number | Auto } Modify the global inode cache size.

option modify tunefstab write_throttle value fs-name Modify the write_throttle parameter value for the specified file system. The parameter write_throttle lets you lower the number of dirty pages per file that the file system generates before writing them to disk. After the number of dirty pages for a file reaches the write_throttle threshold, the file system starts flushing pages to disk even if free memory is still available. The valid range for write_throttle is 0 to 2048 pages. The default value is 0 which implies there is no write_throttle.

option modify tunefstab initial_extent_size value fs-name Modify the initial_extent_size parameter value for the specified file system. The default value for initial_extent_size is 1 file system block. The valid range for initial_extent_size is 1 to 32K blocks and must be the power of 2.
option modify tunefstab read_nstream value fs-name Modify the read_nstream parameter value for the specified file system. The valid range for read_nstream parameter is 1 to number of stripe columns in the associated volume. For the media server workload file system, the recommended read_nstream parameter value is 1.

option modify tunefstab read_pref_io value fs-name Modify the read_pref_io parameter value for the specified file system. The valid values for read_pref_io are 64k, 128k, 256k, or 512k.

option modify tunefstab write_nstream value fs-name Modify the write_nstream parameter value for the specified file system. The valid range for read_nstream parameter is 1 to number of stripe columns in the associated volume.

option modify tunefstab write_pref_io value fs-name Modify the write_pref_io parameter value for the specified file system. The valid values for write_pref_io are 64k, 128k, 256k, or 512k.

option modify dmptune dmp_path_age value Modify the value of dmp_path_age.

option modify dmptune dmp_health_time value Modify the value of dmp_health_time.

stat sys [node] Display system-related statistics.
  stat cluster Display cluster-wide statistics.
  stat dmp [node] Display DMP-related statistics.
  stat all [node] Display system and DMP-related statistics at a time.
  stat rdma [node] Display rdma statistics.

webservices server [start|stop|status] Start, stop, or display the status of the REST server.

webservices SSL certificate certificate_path Set the certificate file of SSL for the REST server.

webservices SSL disable Disable SSL for the REST server.

webservices SSL enable Enable SSL for the REST server.

webservices user password Set the user password. Currently, Veritas Access supports only one user, the manila user.

18.1.4 SEE ALSO

clock(1), ntp(1), option(1), stat(1), webservices(1), license(1), kms(1)
18.2 clock

18.2.1 SYNOPSIS

clock show

clock set time day month year

clock timezone timezone

clock regions [region]

18.2.2 DESCRIPTION

The system clock commands set or show the date and time of the system, including the time zones and the list of regions. Changing cluster time is dangerous and may affect replication, DST, snapshot and other functionalities.

18.2.3 OPTIONS

  clock show  Display the current time and date of the system.

  clock set time day month year  Set the current date and time of the system. The format of time, day, month, and year is given below.

     time : HH:MM:SS using a 24 hour clock
     day : 1..31
     month : January | February | March | April | May | June | July | August | September | October | November | December
     year : YYYY

  clock timezone timezone  Set the timezone to the specified name of the time zone.

  clock regions [region]  Display the list of regions. Regions can be one of the following:

        { Africa, America, Asia, Australia, Canada, Europe, GMT-offset, Pacific, US }

18.2.4 EXAMPLES

Display the current date and time.

    System> clock show
    Mon Jul 13 07:10:39 EDT 2009

Set 1 January 2014 on all the nodes.

    System> clock set 13:00:00 1 January 2014

List all of the timezones in region Asia.

    System> clock regions Asia

Set Calcutta as the timezone.

    System> clock timezone Calcutta
18.2.5 SEE ALSO

ntp(1)
18.3 config

18.3.1 SYNOPSIS

config export local file_name
config export remote URL
config import local file_name [config_type]
   { network|admin|all|report|system|cluster_specific|all_except_cluster_specific|nfs|cifs|ftp|backup|replication|storage_schedules|storage_fs_alert|compress_schedules|defrag_schedules|storage_dedup|smartio }
config import remote URL [config_type]
   { network|admin|all|report|system|cluster_specific|all_except_cluster_specific|nfs|cifs|ftp|backup|replication|storage_schedules|storage_fs_alert|compress_schedules|defrag_schedules|storage_dedup|smartio }
config delete file_name
config list

18.3.2 DESCRIPTION

The system config command imports or exports the Veritas Access configuration settings. The default value: all will be setted if you leave config_type as blank.

<table>
<thead>
<tr>
<th>Config Name</th>
<th>Config information</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>List of users, passwords. This includes cifs local users/groups also.</td>
</tr>
<tr>
<td>network</td>
<td>DNS, LDAP, NIS, netgroup, nsswitch settings (does not include IP).</td>
</tr>
<tr>
<td>report</td>
<td>Report settings.</td>
</tr>
<tr>
<td>system</td>
<td>NTP settings, timezone and system options like cfsmount_ontimeout, dmpio, dmtune, nfsd, ninodes, tunefstab, vxtune.</td>
</tr>
<tr>
<td>all</td>
<td>All the configuration information.</td>
</tr>
<tr>
<td>all_except_cluster_specific</td>
<td>All except the cluster-specific configuration.</td>
</tr>
<tr>
<td>nfs</td>
<td>NFS settings.</td>
</tr>
<tr>
<td>ftp</td>
<td>FTP settings.</td>
</tr>
<tr>
<td>backup</td>
<td>NBU client and NDMP configuration</td>
</tr>
<tr>
<td>cifs</td>
<td>CIFS settings.</td>
</tr>
<tr>
<td>replication</td>
<td>Replication settings.</td>
</tr>
</tbody>
</table>

storage_schedules: Imports dynamic storage tiering (DST) and automated snapshot schedules.

cluster_specific: Public IP addresses, virtual IP addresses, and console IP address. The network connection to the console server may be lost after importing these settings. If this happens, reconnect after importing this configuration.
storage_fs_alert: File system alert settings.
compress_schedules: Compression schedules.
defrag_schedules: Defragmentation schedule.
storage_dedup: File system deduplication settings.
smartio: SmartIO settings.

### 18.3.3 OPTIONS

**config export local file_name**

Save the configuration in a local file.

**config export remote URL**

Save the configuration on a remote machine. Exported File is named export.tar.gz if no file name is specified in the URL. **Note:** When exporting files with ftp URL, the given path is considered relative to the current working directory of the session. For example, to get the file named README from your home directory on your ftp site, use:

```text
ftp://user:passwd@my.site.com/README
```

But if you want to get the README file from the root directory of the site, you need to specify the absolute file name:

```text
ftp://user:passwd@my.site.com//README
```

(i.e. with an extra slash in front of the file name.)

**config import local file_name [config_type] { network | admin | all | report | system | cluster_specific | all_except_cluster_specific | nfs | cifs | ftp | backup | replication | storage_schedules | storage_fs_alert | compress_schedules | defrag_schedules | storage_dedup | smartio }**

Import the specified configuration saved in a local file. **Note** For importing cifs local users/groups you have to import admin module also.

**Warning:** The `config import` command overwrites the existing configuration settings.

**config import remote URL [config_type] { network | admin | all | report | system | cluster_specific | all_except_cluster_specific | nfs | cifs | ftp | backup | replication | storage_schedules | storage_fs_alert | compress_schedules | defrag_schedules | storage_dedup | smartio }**

Import the specified configuration from a remote machine. **Note** For importing cifs local users/groups you have to import admin module also. **Note:** When exporting files with ftp URL, the given path is considered relative to the current working directory of the session. For example, to get the file named README from your home directory on your ftp site, use:

```text
ftp://user:passwd@my.site.com/README
```

But if you want to get the README file from the root directory of the site, you need to specify the absolute file name:

```text
ftp://user:passwd@my.site.com//README
```

(i.e. with an extra slash in front of the file name.)

**config delete file_name**
Delete the locally-saved configuration file.

`config list`

View the list of locally-saved configuration files.

### 18.3.4 EXAMPLES

Export the configuration into a file with the name 2014_July_20.

```
System> config export local 2014_July_20
```

Import only the network configuration.

```
System> config import local 2014_July_20 network
Backup of current configuration was saved as 20140715051522
network configuration was imported
Configuration files are replicated to all the nodes
```

Export (or save) the configuration onto a remote machine.

```
System> config export remote
scp://root@10.209.105.138:/root/2014_July_20.tar.gz
or  ftp://root@10.209.105.138://home/user1/2014_July_20.tar.gz
Password: *******
```

Import the report configuration which is on a remote machine.

```
System> config import remote
ftp://user1@server.com//home/user1/2014_July_20.tar.gz report
Password: *******
```

### 18.3.5 SEE ALSO

`upgrade(1)`
18.4 disable

18.4.1 SYNOPSIS

guidisable

18.4.2 DESCRIPTION

The `guidisable` command disables the GUI.

18.4.3 OPTIONS

- `guidisable` Disable the GUI.

18.4.4 EXAMPLES

Disable the GUI.

```
System> guidisable
Force stopping vamgmt service.
   vamgmt service is not running.
```

18.4.5 SEE ALSO

`guidisable(1)`
18.5 enable

18.5.1 SYNOPSIS

guienenable

18.5.2 DESCRIPTION

The guienenable command enables or starts the GUI.

18.5.3 OPTIONS

    guienenable  Start or enable the GUI.

18.5.4 EXAMPLES

Enable the GUI console.

```
System> guienenable
Start vamgmt service vamgmt...
vamgmt service is running.
```

18.5.5 SEE ALSO

guienenable(1)
18.6 status

18.6.1 SYNOPSIS

guistatus

18.6.2 DESCRIPTION

The guistatus command is used to check the status of the GUI.

18.6.3 OPTIONS

  guistatus  Check the status of the GUI console.

18.6.4 EXAMPLES

Check the status of the GUI console.

System> guistatus
Checking service vamgmt...
vamgmt service is not running.

18.6.5 SEE ALSO

guistatus(1)
18.7 kms

18.7.1 SYNOPSIS

kms config list
kms config status
kms config server server_ip server_port
kms config delete
kms certificate generate
kms certificate import_server_cert
kms certificate import_client_key
kms certificate import_client_cert

18.7.2 DESCRIPTION

The system kms commands are used to register or unregister the cluster with the KMS server.

18.7.3 OPTIONS

kms config list  Display the registered KMS server details.

kms config status  List the status of SSL certificate files that are configured on the cluster.

kms config server server_ip server_port  Register the KMS server with cluster.

kms config delete  Delete the KMS server details.

kms certificate generate  Generate SSL self-signed keypair on cluster. It is advised that cluster nodes' time settings are synchronized with NTP server before generating self-signed certificates.

kms certificate import_server_cert  Import the KMS server's public key.

kms certificate import_client_key  Import the SSL key file of the cluster that is used in CSR.

kms certificate import_client_cert  Import the CA signed public key of the cluster.

18.7.4 EXAMPLES

Display registered KMS server details.

```
System> kms config list
Configured KMS server host: 10.182.65.65
Configured KMS server port: 5696
```

Register KMS server 10.182.65.65 on cluster. Note: We need to import and generate SSL keypair with KMS server certificate file import before running "kms config server" command. KMS servers with OASIS KMIP 1.1 specification are supported.
System> kms config server 10.182.103.113 5696
100% [#] KMS server register with cluster nodes.
ACCESS kms SUCCESS V-288-0 KMS server registered successfully.

Display the configuration status of KMS server communication related SSL certificates.

System> kms config status
ACCESS kms SUCCESS V-288-0 KMS server certificate file imported.

To unregister KMS server on cluster.

System> kms config delete
ACCESS kms SUCCESS V-288-0 Successfully unregistered KMS server.

To generate a self-signed SSL keypair for the cluster.

System> kms certificate generate
ACCESS kms SUCCESS V-288-0 Self-signed certificates successfully generated.

To import the KMS server’s public key on the cluster. Note: We need to generate/import the SSL keypair for the cluster before this operation.

System> kms certificate import_server_cert
Please enter KMS Server certificate details
Please enter KMS Server public key certificate identified by
-----BEGIN CERTIFICATE-----
... (KMS Server certificate in base64 encoding) ... 
-----END CERTIFICATE-----

ACCESS kms SUCCESS V-288-0 Successfully imported KMS server certificate.

To import the cluster’s SSL key file used during CSR creation.

System> kms certificate import_client_key
Please enter client keyfile details

ACCESS kms SUCCESS V-288-0 Successfully imported KMS server certificate.
Enter client's private key identified by
-----BEGIN RSA PRIVATE KEY-----
... (Client key in base64 encoding) ...
-----END RSA PRIVATE KEY-----

-----BEGIN RSA PRIVATE KEY-----
MIIeGcIIBAAKCAQEAncilNq/YBjwEervKIMFwjdXdePxlJjb5Ym0MVG9W+TmGwW
4e47WCXCuZJ29p3jfvQ4HFkJEmz14ARcBrfhh9hivw2z8NF21zUXxHPeuGIqGjmMz
H8bIzA5mkZQL+4WAIUaBzInZd2rQcAYHJYJXk4x03GQq0eU53gIn11QaNT0sDsIQB
hKIftjb+A/KB5Gsfj2JoRdcSn5a16+sx/A1bKL7J6N1YJRR6x2UXHRXlTv9G
Pqc/c1CV8mFtJw4t+oBy1Cbo3bUxGdf1BtEFwhiD2wCt/gQkLzqiCbxqxcGdWjtC
0+BeUwN4wJwXbcJ4qwdAKBZANQYQ2MWCPId1QIDAQAAb0IBADKILTFGaizadaDgNQcK
FRH9JZ0J7F5a5nu/dL8QOi1rOr1DkV0GIlmE3zzGmXcKHln77H8QqXHSWyRYj/yh
ZBKTFzuAmPq49RXKh7tSsm5QzQKEu2mTlUvM6sQFZH1EqOCVJNkJvzXeVTb3
Z5XWq7 seguroVMTfDB5c1cY7t4f1hXy+Glj36d1p0rhyJsw0nqjKCoFqQpLbhXm
IQAfBlzDQbxOMD89N3b30r0y+yj/F31IN1EXhNkbbD1b7/u/umznZ5cEzKlned0
J7GA0M2QQxh210GPAuLqopjpfJl85KX/a4/xSRLA4tN1SRX9B03TkXuwaWU7
qktUe1ckyYEAey6j6tjEsqyYhJxCSoVsi11lnApkY481LBGktUhkYcyCvuFz5AohCuNl
/lQnkke1rxdmboDyc7Bveo9C5GS54PoydOqg9cfXdmr8k9F8Bip9jorPvmEmR2D4
laA8T0cm5GtJGxSnALuuxKws/14S1z1n4vxxhQcgU1F01odHT9kit8CygYEAxiV3
Hj2i2Pr0tOsRrbcCNXLb5tXim9t3fWE1CNSJdoxck0Kz0ZOCMMVxdmFHEQ0G7JAN
RssKStInZtt1TrWdmg1yH1zEcBoKx9eSf2+3rQ53+K9x3iu2Fum5uWy8qg2Ktd
kha61TQxhhr+nsBvMDe4Z2r+1U2t97Gwk4csCgYBKrdkA7zzxWYT6aGbJlZn
8ktvUuUpmVPINzNI1lkxh2x4qUx+6cB03b2d6w4kb57EVeWtgqSqwqAazQ5C4dtz
wlEzepi7Jrdr4kLCcxPfWJ11m5RxmbUHx1d4O1VChYVh7gfaawr+3nutgycQ134
YHjQkc9iGtbn+Unz1s0qQKBgCMjY5DgUz+tBwdsejx5ammdUcmmnPL5TWy18x
DAMW84vzr9z250mOKLQbgq+9zd+17vfAxVISGUh2zVu5MF7swsWeD0+3pqnTR
ixv4s5atkXYPk4VHKBWki91kos65TILuuApeYTOrae3xVAQjQTuFY1NB2tXc
ATbPaGoA27YvRlUT7MNMAe+EO2slJ1l/P0vtnvH5Yw/+0Cv0pvBiyl1Zxaozyq
7R/a9dejEZEcIo7n/tWPgC4L56vBz0+J6EUM2p1TTPuJcMxjP4vnnb7qUumC7M
WXVR1E7gSxqYhexcAkG4SAq0OnPTrnnfxLl6kMhob+qeL705NDk=
-----END RSA PRIVATE KEY-----

ACCESS kms SUCCESS V-288-0 Client key file successfully imported.

To import the cluster’s SSL certificate file signed by CA.

System> kms certificate import_client_key

-----BEGIN CERTIFICATE-----
... (KMS Server certificate in base64 encoding) ...
-----END CERTIFICATE-----
ACCESS kms SUCCESS V-288-0 Successfully imported KMS server certificate.
18.8 license

18.8.1 SYNOPSIS

license add <path_of_key_file>
license list
license list details

18.8.2 DESCRIPTION

The license commands provide options to perform necessary operations related to licensing. It adds or installs a license. It lists the type of license installed on the cluster. It also gives details of the installed license.

18.8.3 OPTIONS

license add <path_of_key_file> Adds or installs the license using the .slf key file which is provided. The scp protocol is also supported for adding license. The scp path should be specified: scp://user@ip:<path_of_key_file>
license list Lists the type of license installed on the cluster. The license type can be trialware (trial license for 60 days), subscription (license with validity of 1 year) or perpetual (permanent license).
license list details Lists the details of the license installed on the cluster such as the product name, version, start date, end date, license type, current state etc.

18.8.4 EXAMPLES

Adding license using local .slf file.

System>license add /home/user1/subscription.slf
ACCESS license SUCCESS V-288-0 License installed successfully on all nodes of the cluster.

Using scp for installing license.

System>license add scp://user1@10.50.148.208:/home/user1/subscription.slf
user1@10.50.148.208's password:
ACCESS license SUCCESS V-288-0 License installed successfully on all nodes of the cluster.

When license installation fails.

System>add /home/user1/key.slf
ACCESS license ERROR V-288-0 Input License file not properly installed on all the nodes; Successfully installed on 0 out of 2 nodes; Installation failure on: ['isaA_01', 'isaA_02']

When an error occurs while fetching the license information.

System>license list
ACCESS license ERROR V-288-0 Could not retrieve license information due to internal error
When a license is installed and the `license list details` command is used.

```
System>license list details
Product Name  Version  Product Edition  License Meter  License Type  Start Date
              End Date  State
============== ======== ================ ============== =============
Veritas Access 7.2.1 ENTERPRISE PER-CORE PERPETUAL NA

When subscription license is installed on the entire cluster

```
System>license list
Installed License Type
=======================
SUBSCRIPTION

System>license list details
Product Name  Version  Product Edition  License Meter  License Type  Start Date
              End Date  State
============== ======== ================ ============== =============
Veritas Access 7.3 ENTERPRISE PER-CORE SUBSCRIPTION 2017-05-25

When the license is installed only on some nodes of the cluster or licensing information from some nodes cannot be fetched as the nodes are down or not reachable.

```
System>license list
Installed License Type
=======================
SUBSCRIPTION

ACCESS license WARNING V-288-0 License is partially installed on this cluster. For more details refer to the Veritas Access GUI.

System>license list details
Product Name  Version  Product Edition  License Meter  License Type  Start Date
              End Date  State
============== ======== ================ ============== =============
Veritas Access 7.3 ENTERPRISE PER-CORE SUBSCRIPTION 2017-05-25

ACCESS license WARNING V-288-0 License is partially installed on this cluster. For more details refer to the Veritas Access GUI.

When a license is not installed on the cluster

```
System>license list
ACCESS license WARNING V-288-0 No license is installed on this cluster.

System>license list details
ACCESS license WARNING V-288-0 No license is installed on this cluster.
18.9 more

18.9.1 SYNOPSIS

more status
more enable
more disable

18.9.2 DESCRIPTION

The system `more` command enables, disables, or checks the status of the more filter. If this command is enabled, then it activates the more filter for paging through text one screen at a time. By default, the more filter is enabled on all of the nodes in the cluster. The more disable command deactivates the more filter on all of the nodes in the cluster.

18.9.3 OPTIONS

more status  Display the status of the more filter.
more enable  Enable the more filter on all of the nodes in the cluster.
more disable  Disable the more filter on all of the nodes in the cluster.

18.9.4 EXAMPLES

Show the status of the more filter.

```
System> more status
Status : Enabled
```

Enable the more filter on all of the nodes.

```
System> more enable
ACCESS more Success V-288-0 more activated on console.
```

Disable the more filter on all of the nodes.

```
System> more disable
ACCESS more Success V-288-0 more deactivated on console.
```
18.10 ntp

18.10.1 SYNOPSIS

ntp show
ntp enable
ntp disable
ntp servername server-name
ntp sync [server-name]

18.10.2 DESCRIPTION

The system `ntp` commands start, stop, synchronize, or check the status of the NTP server.

18.10.3 OPTIONS

- `ntp show` Display the NTP status and server names.
- `ntp enable` Enable NTP on all of the nodes in the cluster.
- `ntp disable` Disable NTP on all of the nodes in the cluster.
- `ntp servername server-name` Set the comma-separated list of NTP servers on all of the nodes in the cluster. Use `127.127.1.0` as the server name to set the local clock.
- `ntp sync [server-name]` Synchronize date with the NTP server on all of the nodes in the cluster.
  
  Note: NTP should be disabled before running the “ntp sync [server name]” command.

18.10.4 EXAMPLES

Display the NTP status and server name.

```
System> ntp show
Status : Disabled
Server Name: 127.127.1.0
```

Set `10.10.10.10` and `20.20.20.20` as the NTP server on all of the nodes.

```
System> ntp servername 10.10.10.10,20.20.20.20
ACCESS System INFO V-288-0 ['10.10.10.10', '20.20.20.20'] has been added into NTP_server.
```

Enable NTP on all of the nodes.

```
System> ntp enable
Enabling the NTP server. Done
```

Disable NTP on all of the nodes.

```
System> ntp disable
Disabling the NTP server. Done
```
Sync date with NTP server on all of the nodes.

```
System> ntp sync
Date is synchronized on all nodes.
```

Sync date with specific NTP server on all of the nodes.

```
System> ntp sync 30.30.30.30
Sync from ['30.30.30.30']...
Date is synchronized on all node.
```

### 18.10.5 SEE ALSO

clock(1)
18.11 option

18.11.1 SYNOPSIS

option show nfsd
option show cfsmount_ontimeout
option show dmpio
option show ninodes
option show tunefstab
option show dmptune
option show vxtune
option show vxfs
option modify nfsd number [nodename]
option modify cfsmount_ontimeout value
option modify dmpio {enclosure enclr_name | arrayname
array_name | arraytype {A/A|A/P|...}
}{iopolicy {adaptive | adaptiveminq | balanced
minimumq | priority | round-robin | singleactive}
option modify ninodes { number | Auto }
option modify tunefstab write_throttle value
option modify dmptune {dmp_path_age value | dmp_health_time value}
option modify vxtune volpagemod_max_memsz value
option modify vxfs vx_timelag value

18.11.2 DESCRIPTION

The system option command is used to display and configure the tunable parameters. The description of the DMP I/O policy is as follows:

adaptive: In SAN environments, determines the paths that have the least delay, and schedules I/O on paths that are expected to carry a higher load. Priorities are assigned to the paths in proportion to the delay.

adaptiveminq: Similar to the adaptive policy, except that I/O is scheduled according to the length of the I/O queue on each path. The path with the shortest queue is assigned the highest priority.

balanced: Takes the track cache into consideration when balancing I/O across paths.

minimumq: Uses a minimum I/O queue policy. I/O is sent on paths that have the minimum number of I/O requests in the queue. This policy is suitable for low-end disks or JBODs where a significant track cache does not exist. This is the default policy for Active/Active (A/A-A) arrays.

priority: Assigns the path with the highest load-carrying capacity as the priority path. This policy is useful when the paths in a SAN have unequal performance, and you want to enforce load-balancing manually.

round-robin: Sets a simple round-robin policy for I/O. This is the default policy for Active/Passive (A/P) and Asynchronous Active/Active (A/A-A) arrays.
singleactive: I/O is channeled through the single active path. The optional attribute use_all_paths controls whether the secondary paths in an Asymmetric Active/Active (A/A-A) array are used for scheduling I/O requests in addition to the primary paths. The default setting is no, which disallows the use of the secondary paths.

18.11.3 OPTIONS

option show nfsd Display the number of NFS daemons for each node in a cluster.

option show cfsmount_ontimeout Display cfsmount online timeout.

option show dmpio Display the type of iopolicy corresponding to enclosure, arrayname, arraytype for each node.

option show ninodes Display the global inode cache size.

option show tunefstab Display the global value of the write_throttle parameter.

option show dmptune Display the value of the dmptune attribute.

option show vxfs Display the tunable parameters for VxFS.

option modify nfsd number [nodename] Modify the number of NFS daemons. The range for the number of daemons is from 1 to 512.

Warning: The modify nfsd command overwrites the existing configuration settings.

option modify cfsmount_ontimeout Value Modify cfsmount online timeout. The range from 300 to 9000.

option modify dmpio {enclosure enclr_name | arrayname} iopolicy{adaptive | adaptiveminq | balanced minimumq | priority | round-robin | singleactive} Modify the dmpio policy corresponding to enclosure, arrayname, arraytype. Warning: Check the sequence before modifying the I/O policy. The policies need to be applied in the following sequence: arraytype, arrayname, and enclosure. The enclosure-based modification of the I/O policy overwrites the I/O policy set using the arrayname and the arraytype for that particular enclosure. In turn, the arrayname-based modification of the I/O policy overwrites the I/O policy set using the arraytype for that particular arrayname.

option modify tunefstab write_throttle value Modify the value of the write_throttle parameter.

option modify dmptune dmp_health_time value Modify the value of dmp_health_time. This attribute sets the time in seconds for which a path must stay healthy. If a path’s state changes back from enabled to disabled within this time period, DMP marks the path as intermittently failing, and does not re-enable the path for I/O until dmp_path_age seconds elapse. The default value of dmp_health_time is 60 seconds. A value of 0 prevents DMP from detecting intermittently failing paths.

option modify dmptune dmp_path_age value Modify the value of dmp_path_age. The time for which an intermittently failing path needs to be monitored before DMP marks the path as healthy and once again attempts to schedule I/O requests on it. The default value is 300 seconds. A value of 0 prevents DMP from detecting intermittently failing paths.

option modify ninodes {number | Auto} Modify the global inode cache size. The range for inode cache size is from 10000 to 8000000. Set to Auto to enable autoreset by VXFS.

Warning: The modify ninodes command requires a cluster-wide reboot.
**option modify vxtune volpagemod_max_memsz value**

Modify the value of volpagemod_max_memsz. This is the maximum memory measured in kilobytes that is allocated for cache object metadata. The default value for volpagemod_max_memsz is set to 131072KB. The value that should be used is determined by the total size of volumes for which instant rollbacks are to be taken. The following formula can be used to calculate the required value of volpagemod_max_memsz:

\[ \text{size}_\text{in KB} = 6 \times (\text{total}_\text{filesystem}_\text{size}_\text{in GB}) \times (64/\text{region}_\text{size}_\text{in KB}) \]

The region_size can be set to 256KB by default for large filesystems.

**option modify vxfs vx_timelag value**

Modify the values of vx_ifree_timelag and vx_iclean_timelag.

-vx_ifree_timelag

VxFS maintains an inode free list. If you configure the vx_ifree_timelag value as 30 seconds, the freelist is scanned every 30 seconds.

-vx_iclean_timelag

This is the minimum time that an inode must be in the inode free list before the system reclaims it. VALUE Specify an integer value (Unit: Seconds)

### 18.11.4 EXAMPLES

Show the value of the number of NFS daemons.

```
System> option show nfsd
NODENAME NUMBER_DAEMONS
------- --------------
sfs_01 66
```

Show cfsmount online timeout.

```
System> option show cfsmount_ontimeout
Resource OnlineTimeout
-------- --------------
 cfsmount 300
```

Show the value of dmpio policy corresponding to enclosure, arrayname, arraytype.

```
System> option show dmpio
NODENAME TYPE ENCLR/ARRAY IOPOLICY
------- ------- -------------- -------
sfs_01 enclosure disk Balanced
sfs_01 enclosure aluadisk0 Priority
sfs_01 arraytype A/A balanced
sfs_02 enclosure disk Balanced
sfs_02 enclosure aluadisk0 Priority
sfs_02 arraytype A/A balanced
```

Show the value of the global inode cache size.

```
System> option show ninodes
INODE_CACHE_SIZE
----------------
565580
```
Show the value of the `tunefstab` parameters.

<table>
<thead>
<tr>
<th>NODENAME</th>
<th>ATTRIBUTE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfs_01</td>
<td>write_throttle</td>
<td>0</td>
</tr>
</tbody>
</table>

Show the value of the `dmptune` parameters.

<table>
<thead>
<tr>
<th>NODENAME</th>
<th>ATTRIBUTE</th>
<th>VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfs_01</td>
<td>dmp_path_age</td>
<td>57</td>
</tr>
<tr>
<td>sfs_01</td>
<td>dmp_health_time</td>
<td>44</td>
</tr>
</tbody>
</table>

Show the value of the `vxtune` parameters.

<table>
<thead>
<tr>
<th>NODENAME</th>
<th>TUNABLE</th>
<th>VALUE (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>sfs_01</td>
<td>volpagemod_max_memsz</td>
<td>12288</td>
</tr>
<tr>
<td>sfs_02</td>
<td>volpagemod_max_memsz</td>
<td>12288</td>
</tr>
</tbody>
</table>

Modify the number of NFS daemons on all the nodes in a cluster.

System> option modify nfsd 97

Modify `cfsmount online timeout`.

System> option modify cfsmount_ontimeout 400

Modify the `dmpio policy`, `enclosure`, and `diskname`.

System> option modify dmpio enclosure Disk Balanced

Modify the global `inode cache size`.

System> option modify ninodes 2000343

Enable `inode cache size autoreset`.

System> option modify ninodes Auto

Modify the `write_throttle` parameter of `tunefstab`.

System> option modify tunefstab write_throttle 20003

Modify the `dmp_path_age` parameter of `dmptune`.

System> option modify dmptune dmp_path_age 40

Modify the `dmp_health_time` parameter of `dmptune`.

System> option modify dmptune dmp_health_time 50

Modify the `volpagemod_max_memsz` parameter of `vxtune`
18.11.5 SEE ALSO

clock(1), ntp(1), stat(1), swap(1)
18.12 stat

18.12.1 SYNOPSIS

stat sys [node]
stat dmp [node]
stat fsio [fsname]
stat cluster
stat all [node]
stat rdma [node]

18.12.2 DESCRIPTION

System stat command displays the system, DMP, and process-related node-wide statistics. The load in the displayed output is the load from the last 1, 5, and 15 minutes. Intr is the total number of interrupt counts, and ctxt is the total number of context switches that occurred after a reboot.

The stat command cluster option displays I/O and network throughput at the entire cluster level.

18.12.3 OPTIONS

stat sys [node]
    Display system-related statistics. node : name of a node in the cluster.

stat dmp [node]
    Display DMP-related statistics. node : name of a node in the cluster.

stat fsio [fsname]
    Display filesystem IO statistics. fsname : name of the filesystem.

stat cluster
    Display cluster IO and network throughput.

stat all [node]
    Display system and DMP-related statistics of all the nodes or a node in the cluster at a time. node : name of a node in the cluster.

stat rdma [node]
    Display RDMA statistics of all the nodes or specific node(s) in the cluster at a time. node : name of node(s) in the cluster.

18.12.4 EXAMPLES

Display system-related statistics of node1.

System> stat sys node1
Gathering statistics...
GEN STAT :::
============
CPU Idle : 99.450    Load 1 : 1.020
Display consolidated system-related statistics of all running nodes in the cluster.

```
System> stat sys
Gathering statistics...
Node %cpu_util %mem_util av_read_time(ms) av_write_time(ms) rx_av_pubeth(mb/s)
     tx_av_pubeth(mb/s)
node1  0.800  49.680  0.000   0.000     0.000                        0.
node2  0.150  50.110  0.000   0.000     0.000                        0.
```

Display DMP-related statistics of node1.

```
System> stat dmp node1
DMP STAT :::
==============
OPERATIONS KBYTES AVG TIME(ms)
PATHNAME READS WRITES READS WRITES READS WRITES
sda 978 0 0 0 0 0.0 0.0
sdf 477 0 0 0 0 0.0 0.0
sdd 457 0 0 0 0 0.0 0.0
sdg 3043 0 0 0 0 0.0 0.0
sde 6096 0 0 0 0 0.0 0.0
```

Display consolidated DMP-related statistics of all the running nodes in the cluster.

```
System> stat dmp
DMP STAT :::
==============
OPERATIONS KBYTES AVG TIME(ms)
PATHNAME READS WRITES READS WRITES READS WRITES
sda 978 0 0 0 0 0.0 0.0
sdf 477 0 0 0 0 0.0 0.0
sdd 457 0 0 0 0 0.0 0.0
sdg 3043 0 0 0 0 0.0 0.0
sde 6096 0 0 0 0 0.0 0.0
```
Display filesystem IO statistics of all running nodes in the cluster.

```
System> stat fsio testfs1

OPERATIONS BLOCKS AVG TIME(ms)
NAME READ WRITE READ WRITE READ WRITE
---- --------------- --------------- ------------
Node: sfs1_0
==============
testfs1_tier1 532 206 2336 7486 1.17 9.98
testfs1_tier2 1 1 2 16 4.00 8.00
Node: sfs1_1
==============
testfs1_tier1 369 168 1970 3218 2.12 7.67
testfs1_tier2 1 0 2 0 0.00 0.00
```

Display system and DMP-related statistics of node1.

```
System> stat all node1
```

Display system and DMP-related statistics of all nodes in the cluster.

```
System> stat all
```

Display cluster wide Network and IO throughput.

```
System> stat cluster
Gathering statistics...
Cluster wide statistics::::
==================================
IO throughput :: 0
Network throughput :: 1.205
```

Display RDMA network statistics.

```
System> stat rdma
Gathering statistics...
TAG-NAME MODE PRIORITY MTU BROADCAST TxPKTS (M) TxBYTES (MB) RxPKTS
========== ===== ========= ==== =========== =========== =========
priveth0 rdma hipri 8192 172.16.0.255 1.45 106.35 1.34
priveth1 rdma hipri 8192 172.16.1.255 1.45 106.35 1.34
```

Display RDMA network statistics for specific node(s).

```
System> stat rdma rdma_01,rdma_02
Gathering statistics...
NODE TAG-NAME PROTOCOL NODE-RANGE LINK-TYPE UDP-PORT MTU IP ADDRESS ...
  BCAST ADDRESS
```

18.12. stat
<table>
<thead>
<tr>
<th>Node</th>
<th>Interface</th>
<th>Protocol</th>
<th>Port</th>
<th>Address 1</th>
<th>Address 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>rdma_02</td>
<td>priveth0</td>
<td>udp</td>
<td>51001</td>
<td>172.16.0.4</td>
<td>172.16.0.255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdma_02</td>
<td>priveth1</td>
<td>udp</td>
<td>51002</td>
<td>172.16.1.4</td>
<td>172.16.1.255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdma_01</td>
<td>priveth0</td>
<td>udp</td>
<td>51001</td>
<td>172.16.0.3</td>
<td>172.16.0.255</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rdma_01</td>
<td>priveth1</td>
<td>udp</td>
<td>51002</td>
<td>172.16.1.3</td>
<td>172.16.1.255</td>
</tr>
</tbody>
</table>

NOTE: MTU: ‘-’ is the default, which has a value of 8192. NODE-RANGE: ‘-‘ indicates all cluster are to be configured for this link.
18.13 webservices

18.13.1 SYNOPSIS

webservices server [start|stop|status]
webservices SSL certificate certificate_path
webservices SSL disable
webservices SSL enable
webservices user password

18.13.2 DESCRIPTION

The system webservices commands allow you to maintain the REST server. You can start, stop, or display the status of the REST server. You can also enable, disable, or set the SSL certificate for the REST server. You can also change the password of the REST server user.

18.13.3 OPTIONS

   certificate Certificate file path and name. Make sure to set the correct read permissions for the certificate file.
   server [start|stop|status] Start, stop, or display the status of the REST server.
   SSL certificate certificate_path Set the certificate file of SSL for the REST server.
   SSL disable Disable SSL for the REST server.
   SSL enable Enable SSL for the REST server.
   user password Set the user password. Currently, Veritas Access supports only one user, the manila user.

18.13.4 EXAMPLES

Start the REST server.

System> webservices server start
ACCESS REST SUCCESS V-288-1397 REST server is started.

Display the status of the REST server.

System> webservices server status
Certificate : /opt/VRTSnas/conf/ssl.pem
User : manila
SSL : disable
Status : ONLINE

Stop the REST server.

System> webservices server stop
ACCESS REST SUCCESS V-288-1397 REST server is stopped.
Set the certificate file for the REST server.

```
System> webservice SSL certificate /opt/VRTSnas/conf/ssl.pem
ACCESS REST SUCCESS V-288-1397 Set REST server certificate successfully.
```

Disable SSL for the REST server.

```
System> webservice SSL disable
ACCESS REST SUCCESS V-288-1397 REST server SSL disabled.
```

Enable SSL for the REST server.

```
System> webservice SSL enable
ACCESS REST SUCCESS V-288-1397 REST server SSL enabled.
```

Set user “manila” password.

```
System> webservice user password
Changing password for manila
Old password:
New password:
Re-enter new password:
ACCESS REST SUCCESS V-288-1397 REST server user password changed.
```

18.13.5 SEE ALSO
19.1 target

19.1.1 SYNOPSIS

iscsi service start
iscsi service stop
iscsi service status
iscsi target create
iscsi target auth incominguser add
iscsi target auth incominguser delete
iscsi target destroy
iscsi target list [targetname]
iscsi target portal add
iscsi target portal delete
iscsi lun create [lun-name] [lunid] [target-name] [size]
iscsi lun list
iscsi lun list [targetname]
iscsi lun destroy [lunid] [target-name]
iscsi target status [*target-name*]
iscsi target map add [initiator-name] [target-name]
iscsi target map delete [initiator-name] [target-name]
iscsi target store add [fs-name] [target-name]
iscsi target store delete [fs-name] [target-name]
19.1.2 DESCRIPTION

The iscsi target command monitors and modifies Linux SCSI target software like targets, volumes, etc. The auth incominguser commands maintains iscsi CHAP authentication. An authentication is required before an initiator is allowed to log in and access devices. CHAP main-phase authentication is set on the target level. To set up CHAP authentication:

1. Create a target.
2. Create an account and an associated password.
3. Bind the account to one or more targets.
4. Check the status of a specific iSCSI target.

The iscsi lun commands are used to perform LUN related operations on a file system. The iscsi target map commands deal with the mapping of initiator name to specified iscsi target. The iscsi target store commands deal with addition and deletion of store which is a file system.

19.1.3 OPTIONS

iscsi service start  Start the iSCSI target service.
iscsi service stop   Stop the iSCSI target service.
iscsi service status Check the status of the iSCSI target service.
iscsi target create  Create an iSCSI target.
iscsi target auth incominguser add Create an incoming user and bind the account to specific, existing iSCSI target.
iscsi target auth incominguser delete Remove an incoming user and unbind the account from its corresponding iSCSI target.
iscsi target destroy Destroy a specific iSCSI target.
iscsi target list [targetname]  List all or specific iSCSI targets.
iscsi target portal add  Add the portal address for an iSCSI target service.
iscsi target portal del Delete the portal address for an iSCSI target service.
iscsi lun create [lun-name] [lunid] [target-name] [size]  Create a LUN with the specified name, LUN ID and size.
target iscsi lun list List the details of all the LUNs present on the system for all the targets.
target iscsi lun list [targetname]  List details of the information of this LUN which is mapped to given target.
target iscsi lun destroy [lunid] [target-name]  Destroy a specific LUN.
iscsi target status [targetname]  Check the status of a specific iSCSI target.
iscsi target map add [initiator-name] [target-name]  Map the iSCSI initiator with specified iSCSI target.
iscsi target map delete [initiator-name] [target-name]  Remove the iSCSI initiator mapped to a specified iSCSI target.
iscsi target store add [fs-name] [target-name]  Map fs with specified iSCSI target.
**iscsi target store delete [fs-name] [target-name]** Remove the fs from specified iSCSI target.

### 19.1.4 EXAMPLES

Start the iSCSI target service. If the iSCSI target service is already started, the start command clears the faults, if any, and then tries to start the iSCSI target service:

```
Target> iscsi service start
ACCESS Target SUCCESS V-288-0 iSCSI Target service started
```

Stop the iSCSI target service:

```
Target> iscsi service stop
ACCESS Target SUCCESS V-288-0 iSCSI Target service stopped
```

Check the status of iSCSI target service:

```
Target> iscsi service status
Node     Status
VA_01    OFFLINE
VA_02    OFFLINE
```

Create an iSCSI target:

```
Target> iscsi target create iqn.2017-02.com.veritas:target03
```

Create an incoming user and bind the account to specific, existing iSCSI target:

```
Target> iscsi target auth incominguser add robin robin iqn.2017-02.com.veritas:target03
ACCESS Target SUCCESS V-288-0 Add user robin successfully.
```

Remove an incoming user and unbind the account from its corresponding iSCSI target:

```
Target> iscsi target auth incominguser delete robin target1
ACCESS Target SUCCESS V-288-0 Delete user robin successfully.
```

Destroy a specific iSCSI target:

```
Target> iscsi target destroy iqn.2001-04.com.veritas:target2
ACCESS Target SUCCESS V-288-0 iSCSI target deletion for iqn.2001-04.com.veritas:target2 was completed successfully.
```

List all or specific iSCSI target:

```
 Target> iscsi target list
Target Name Target Id Parent Node Accounts
 == =================================== =============== ===========
 iqn.2001-04.com.veritas:target1 1 VA_01       ['user1', 'user2']
 iqn.2001-04.com.veritas:target2 2 VA_01       []
```

Add the portal address for an iSCSI target service:

```
19.1. target
```
Target> iscsi target portal add 192.168.10.32
ACCESS Target SUCCESS V-288-0 Portal add successful. Start the iSCSI service for the portal address to take effect.

Delete the portal address for an iSCSI target service:

Target> iscsi target portal del
ACCESS Target SUCCESS V-288-0 Portal IP deleted successfully

Create a LUN with the specified name, LUN ID and size:

Target> iscsi lun create lun3 3 iqn.2017-03.com.veritas:atarget1 200m
ACCESS Target SUCCESS V-288-0 Lun lun3 created successfully and added to target iqn.2017-03.com.veritas:atarget1

List the details of all the LUNs present on the system for all the targets:

```
Target> iscsi lun list
Target Name Lun Name Lun ID Lun Size
------------------------------- ---------- ---- ----
  iqn.2017-02.com.veritas:target2 lun_1   21  10M
  iqn.2017-02.com.veritas:target2 lun_2   22  10M
  iqn.2017-02.com.veritas:target2 lun_3   23  10M
```

List the details of the LUNs which are mapped to a specified target:

```
Target> iscsi lun list iqn.2017-02.com.veritas:target1
Lun Name Lun ID Lun Size Store
--------- --------- -------- ------
  lun1      12       2M /vx/fs1/12
  lun2      13       2M /vx/fs1/13
  lun3      14       2k /vx/fs1/14
```

Destroy a specific LUN:

```
isaA> target iscsi lun destroy 4 iqn.2017-02.com.veritas:target2
ACCESS Target SUCCESS V-288-0 Lun deletion for lun id 4 was successful.
```

Check the status of a specific iSCSI target:

```
Target> iscsi target status iqn.2017-10.com.veritas:target11
ACCESS Target SUCCESS V-288-0 Status of target iqn.2017-10.com.veritas:target11 is__ONLINE
```

Map an iSCSI initiator with specific iSCSI target:

```
```

Remove the mapping of iSCSI initiator from specific iSCSI target:

```
```
Map the store to specific iSCSI target:

```
Target> iscsi target store add fs3 iqn.2017-02.com.veritas:target1
```

Remove the mapping of store from specific iSCSI target:

```
Target> iscsi target store delete fs3 iqn.2017-02.com.veritas:target1
```

19.1.5 SEE ALSO

target_iscsi_lun(1), target_iscsi_service(1), target_iscsi_target(1)
19.2 iscsi lun

19.2.1 SYNOPSIS

iscsi lun create [lun-name] [lunid] [target-name] [size]
iscsi lun list
iscsi lun list [targetname]
iscsi lun destroy [lunid] [target-name]

19.2.2 DESCRIPTION

The iscsi lun commands are used to perform LUN-related operations.

19.2.3 OPTIONS

iscsi lun create [lun-name] [lunid] [target-name] [size] Create a LUN with the specified name, LUN ID, and size.
target iscsi lun list List the details of all the LUNs present on the system for all the targets.
target iscsi lun list [targetname] List the details of the LUNs which are mapped to a specified target.
target iscsi lun destroy [lunid] [target-name] Destroy a specific LUN.

19.2.4 EXAMPLES

Create a LUN with the specified name, LUN ID, and size:

```bash
Target> iscsi lun create lun3 3 iqn.2017-03.com.veritas:atarget1 200m
ACCESS Target SUCCESS V-288-0 Lun lun3 created successfully and added to target iqn.2017-03.com.veritas:atarget1
```

List the details of all the LUNs present on the system for all the targets:

```
Target> iscsi lun list

Target Name Lun Name Lun ID Lun Size
------------------------------- ------------- -------------
iqn.2017-02.com.veritas:target2 lun_1 21 10M
iqn.2017-02.com.veritas:target2 lun_2 22 10M
iqn.2017-02.com.veritas:target2 lun_3 23 10M
```

List the details of the LUNs which are mapped to a specified target:

```
Target> iscsi lun list iqn.2017-02.com.veritas:target1

Lun Name Lun ID Lun Size Store
-------- ------- ------- ------------
lun1 12 2M /vx/fs1/12
lun2 13 2M /vx/fs1/13
lun3 14 2k /vx/fs1/14
```

Destroy a specific LUN:
Veritas Access Command Reference Guide Documentation, Release 7.3

19.2.5 SEE ALSO

target(1), target_iscsi_service(1), target_iscsi_target(1)
19.3 iscsi target service

19.3.1 SYNOPSIS

iscsi service start
iscsi service stop
iscsi service status

19.3.2 OPTIONS

    iscsi service start  Start the iSCSI target service.
    iscsi service stop   Stop the iSCSI target service.
    iscsi service status Check the status of the iSCSI target service.

19.3.3 EXAMPLES

Start the iSCSI target service. If the iSCSI target service is already started, the start command clears the faults, if any, and then tries to start the iSCSI target service:

    Target> iscsi service start
    ACCESS Target SUCCESS V-288-0 iSCSI Target service started

Stop the iSCSI target service:

    Target> iscsi service stop
    ACCESS Target SUCCESS V-288-0 iSCSI Target service stopped

Check the status of iSCSI target service:

    Target> iscsi service status
    Node  Status
    ====== ========
    VA_01  OFFLINE
    VA_02  OFFLINE

19.3.4 SEE ALSO

target(1), target_iscsi_lun(1), target_iscsi_target(1)
19.4 iscsi target

19.4.1 SYNOPSIS

iscsi target create
iscsi target auth incominguser add
iscsi target auth incominguser delete
iscsi target destroy
iscsi target list [targetname]
iscsi target status [targetname]
iscsi target map add [initiator-name] [target-name]
iscsi target map delete [initiator-name] [target-name]
iscsi target store add [fs-name] [target-name]
iscsi target store delete [fs-name] [target-name]
iscsi target portal add [ip-address]
iscsi target portal del

19.4.2 DESCRIPTION

The auth incominguser commands maintain ISCSI CHAP authentication. CHAP main-phase authentication is set on the target level.

The iscsi target map commands deal with the mapping of initiator name to specified iscsi target. The iscsi target store commands deal with addition and deletion of store which is a file system. The iscsi target portal commands deal with the addition and deletion of portal ip-address.

19.4.3 OPTIONS

iscsi target create Create an iSCSI target.
iscsi target auth incominguser add Create an incoming user and bind the account to specific, existing iSCSI target.
iscsi target auth incominguser delete Remove an incoming user and unbind the account from its corresponding iSCSI target.
iscsi target destroy Destroy a specific iSCSI target.
iscsi target list [targetname] List all or specific iSCSI targets.
iscsi target status [targetname] Check the status of a specific iSCSI target.
iscsi target map add [initiator-name] [target-name] Map the iSCSI initiator with specified iSCSI target.
iscsi target map delete [initiator-name] [target-name] Remove the iSCSI initiator mapped to a specified iSCSI target.
iscsi target store add [fs-name] [target-name] Map fs with specified iSCSI target.
Veritas Access Command Reference Guide Documentation, Release 7.3

**iscsi target store delete [fs-name] [target-name]** Remove the fs from specified iSCSI target.

**iscsi target portal add [ip-address]** Add portal ip-address.

**iscsi target portal del** Remove portal ip-address.

### 19.4.4 EXAMPLES

Create an iSCSI target:

```
Target> iscsi target create iqn.2017-02.com.veritas:target03
```

Create an incoming user and bind the account to specific, existing iSCSI target:

```
Target> iscsi target auth incominguser add robin robin iqn.2017-02.com.veritas:target03
ACCESS Target SUCCESS V-288-0 Add user robin successfully.
```

Remove an incoming user and unbind the account from its corresponding iSCSI target:

```
Target> iscsi target auth incominguser delete robin iqn.2001-04.com.veritas:target2
ACCESS Target SUCCESS V-288-0 Delete user robin successfully.
```

Destroy a specific iSCSI target:

```
Target> iscsi target destroy iqn.2001-04.com.veritas:target2
ACCESS Target SUCCESS V-288-0 iSCSI target deletion for iqn.2001-04.com.veritas:target2 was completed successfully.
```

List all or specific iSCSI target:

```
Target> iscsi target list
Target Name Target Id Store
================================
qn.2017-02.com.veritas:target1 1 fs1
qn.2017-02.com.veritas:target2 2
qn.2017-02.com.veritas:target3 3

Target> iscsi target list iqn.2017-02.com.veritas:target1
Target Name Target Id Store Accounts Initiator Mappings
================================
qn.2017-02.com.veritas:target1 1 fs1 user_1, user_2 iqn.2001-04.com.veritas:40274.01
```

Check the status of a specific iSCSI target:

```
Target> iscsi target status iqn.2017-10.com.veritas:target11
ACCESS Target SUCCESS V-288-0 Status of target iqn.2017-10.com.veritas:target11 is ONLINE
```

Map an iSCSI initiator with specific iSCSI target:

```
```
Remove the mapping of iSCSI initiator from specific iSCSI target:

```
ACCESS Target SUCCESS V-288-0 Remove initiator iqn.2001-04.com.veritas:26064.01
   -> mapping from target iqn.2017-02.com.veritas:target1 successfully
```

Map the store to specific iSCSI target:

```
Target> iscsi target store add fs3 iqn.2017-02.com.veritas:target1
```

Remove the mapping of store from specific iSCSI target:

```
Target> iscsi target store delete fs3 iqn.2017-02.com.veritas:target1
```

Add a portal ip-address:

```
Target> iscsi target portal add 192.168.10.38
ACCESS Target SUCCESS V-288-0 Portal add successful. Start the iSCSI service for the
   -> portal address to take effect.
```

Remove the portal ip-address:

```
Target> iscsi target portal del
ACCESS Target SUCCESS V-288-0 Portal IP deleted successfully.
```

### 19.4.5 SEE ALSO

target(1), target_iscsi_lun(1), target_iscsi_service(1)
20.1 upgrade

20.1.1 SYNOPSIS

version
history
repository
get URL
install version

20.1.2 DESCRIPTION

The upgrade commands install patches to the Veritas Access software. The software is installed on all the nodes. The upgrade version command also shows the current software version.

20.1.3 OPTIONS

version Displays the current running version of Veritas Access software.
history Displays the upgrade history of Veritas Access software.
repository Display all releases that are available in the repository.
get URL Downloads the release and puts it in the repository.
install version Upgrade the cluster to the specified version.

20.1.4 EXAMPLES

Displays the current running version of Veritas Access software:

```
Upgrade> version
ACCESS 7.1.0.0   (Fri Mar 11 12:49:05 2016)
```
Displays the upgrade history of Veritas Access software:

Upgrade> history
ACCESS 7.0.0.0  (Thu November 8 00:00:00 CST 2015), Installed on Fri Sep 19 00:00:00 CST 2015
ACCESS 7.1.0.0  (Mon Jul 7 00:00:00 CST 2015), Installed on Fri Sep 19 00:00:00 CST 2015

Download a patch from an HTTP server with authentication:

Upgrade> get http://admin8docserver.veritas.com/patches/ACCESS.tar.gz
Enter password for user 'admin': **********
ACCESS upgrade NOTICE V-288-0 ACCESS patch downloaded and stored in repository.

Display all releases that are available in the repository:

Upgrade> repository
ACCESS VERSION| INSTALLED(y/n)| UPGRADABLE(y/n)
7.1.0.1     y       n
7.1.0.2     n       y
7.2.0.0     n       y

Upgrade the cluster to the specified version:

Upgrade> install 6.0.0.2
Veritas Veritas Access 6.0.0.2 Upgrade Program

20.1.5 SEE ALSO

get(1), history(1), install(1), repository(1), version(1)
20.2 get

20.2.1 SYNOPSIS

get URL

20.2.2 DESCRIPTION

The upgrade get URL command downloads the release and puts it in the repository.

20.2.3 OPTIONS

get URL  The command downloads the patch release from the URL and put it in the repository. It also validates the patch release downloaded and shows error if the downloaded release is not valid. The URL is the URL location from where you can download the software patch. The URL supports HTTP, FTP, and SCP protocols for download. The user name and password for the HTTP and FTP protocols are also supported.

20.2.4 EXAMPLES

Downloads the release and puts it in the repository:

```
Upgrade> get http://admin@docserver.veritas.com/patches/ACCESS.tar.gz
Enter password for user 'admin': **********
ACCESS upgrade NOTICE V-288-0 ACCESS patch downloaded and stored in repository.

Upgrade> get scp://root@10.198.89.178:/patches/ACCESS.tar.gz
Enter password for user 'root': **********
ACCESS upgrade NOTICE V-288-0 ACCESS patch downloaded and stored in repository.
```

20.2.5 SEE ALSO

patch(1)
20.3 history

20.3.1 SYNOPSIS

history

20.3.2 DESCRIPTION

The upgrade history command displays the upgrade history of Veritas Access software.

20.3.3 OPTIONS

history Displays the upgrade history of Veritas Access software, including the ACCESS software release date, the ACCESS software upgrade history. It also shows error messages if any of the nodes do not have matching software versions installed.

20.3.4 EXAMPLES

Displays the upgrade history of Veritas Access software:

```
Upgrade> history
ACCESS 7.0.0.0 (Thu November 8 00:00:00 CST 2015), Installed on Fri Sep 19 00:00:00 CST 2015
ACCESS 7.1.0.0 (Mon Jul 7 00:00:00 CST 2015), Installed on Fri Sep 19 00:00:00 CST 2015
```

20.3.5 SEE ALSO

patch(1)
20.4 install

20.4.1 SYNOPSIS

install version

20.4.2 DESCRIPTION

The upgrade install version command upgrade the cluster to the specified version.

20.4.3 OPTIONS

install version  The ACCESS upgrade install commands perform a direct upgrade or a guided rolling upgrade on all of the clusters nodes based on the patch type. Before you perform an upgrade, ensure that all the cluster nodes are in RUNNING state and have the same Veritas Access software version.

20.4.4 EXAMPLES

Upgrade the cluster to the specified version:

```
Upgrade> install 7.1.0.2
Veritas Veritas Access 7.1.0.2 Upgrade Program
```

20.4.5 SEE ALSO

patch(1)
20.5 repository

20.5.1 SYNOPSIS

repository

20.5.2 DESCRIPTION

The upgrade repository command displays all releases that are available in the repository.

20.5.3 OPTIONS

repository Displays all releases that are available in the repository. It also shows if a patch release in the repository is installed or not, or the patch release can be used to upgrade the cluster.

20.5.4 EXAMPLES

Display all releases that are available in the repository:

```
Upgrade> repository

<table>
<thead>
<tr>
<th>ACCESS VERSION</th>
<th>INSTALLED(y/n)</th>
<th>UPGRADABLE(y/n)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1.0.1</td>
<td>y</td>
<td>n</td>
</tr>
<tr>
<td>7.1.0.2</td>
<td>n</td>
<td>y</td>
</tr>
<tr>
<td>7.2.0.0</td>
<td>n</td>
<td>y</td>
</tr>
</tbody>
</table>
```

20.5.5 SEE ALSO

patch(1)
20.6 version

20.6.1 SYNOPSIS

version

20.6.2 DESCRIPTION

The upgrade version command displays the current running version of Veritas Access software.

20.6.3 OPTIONS

version Displays the current running version of Veritas Access software, including the ACCESS software release date. It also shows error messages if any of the nodes do not have matching software versions installed.

20.6.4 EXAMPLES

Displays the current running version of Veritas Access software:

```
Upgrade> version
ACCESS 7.2.1.0     (Fri Mar 11 12:49:05 2016)
```

20.6.5 SEE ALSO

patch(1)