

# Veritas Access 7.2 Command-Line Administrator's Guide

Linux

# Veritas Access Administrator's Guide

Last updated: 2016-11-21

Document version: 7.2 Rev 1

## Legal Notice

Copyright © 2016 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

<http://www.veritas.com>

## Technical Support

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

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

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

<https://my.veritas.com>

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

Worldwide (except Japan)

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

Japan

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

## Documentation

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

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

## Documentation feedback

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

[doc.feedback@veritas.com](mailto:doc.feedback@veritas.com)

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

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

# Contents

<b>Section 1</b>	<b>Introducing Veritas Access</b> .....	17
<b>Chapter 1</b>	<b>Introducing Veritas Access</b> .....	18
	About Veritas Access .....	18
<b>Chapter 2</b>	<b>Getting started with the Veritas Access command-line interface</b> .....	22
	Logging on to Veritas Access .....	23
	Using the Veritas Access CLI .....	23
	Adding Master, System Administrator, and Storage Administrator users .....	24
	About user roles and privileges .....	27
	About the naming requirements for adding new users .....	27
	Displaying the command history .....	28
	Using the more command .....	29
	Getting help using the Veritas Access command-line interface .....	30
<b>Section 2</b>	<b>Configuring Veritas Access</b> .....	33
<b>Chapter 3</b>	<b>Configuring the Veritas Access network</b> .....	34
	About configuring the Veritas Access network .....	35
	Displaying the network configuration and statistics .....	35
	About bonding Ethernet interfaces .....	37
	Bonding Ethernet interfaces .....	39
	Understanding private NIC bonding .....	42
	Configuring DNS settings .....	44
	About the IP addresses for the Ethernet interfaces .....	47
	About Ethernet interfaces .....	48
	Configuring IP addresses .....	48
	Configuring Veritas Access to use jumbo frames .....	54
	Displaying current Ethernet interfaces and states .....	55
	Configuring Ethernet interfaces .....	56
	Configuring VLAN interfaces .....	57

	Configuring NIC devices .....	59
	Monitoring NIC devices using IP addresses .....	62
	Swapping network interfaces .....	63
	Excluding PCI IDs from the cluster .....	65
	About configuring routing tables .....	67
	Configuring routing tables .....	68
<b>Chapter 4</b>	<b>Configuring authentication services .....</b>	<b>74</b>
	About configuring LDAP settings .....	74
	Configuring LDAP server settings .....	75
	Administering the Veritas Access cluster's LDAP client .....	79
	Configuring the NIS-related settings .....	81
	Configuring NSS lookup order .....	83
<b>Chapter 5</b>	<b>Configuring system information .....</b>	<b>85</b>
	Coordinating cluster nodes to work with NTP servers .....	85
	Setting the system clock .....	89
<b>Section 3</b>	<b>Managing storage .....</b>	<b>92</b>
<b>Chapter 6</b>	<b>Configuring storage .....</b>	<b>93</b>
	About storage provisioning and management .....	93
	About Flexible Storage Sharing .....	94
	Limitations of Flexible Storage Sharing .....	95
	Displaying information for all disk devices associated with the nodes in a cluster .....	95
	Configuring disks .....	98
	Increasing the storage capacity of a LUN .....	100
	Formatting or reinitializing a disk .....	101
	Removing a disk .....	101
	Displaying WWN information .....	102
	Initiating host discovery of LUNs .....	104
	Importing new LUNs forcefully for new or existing pools .....	104
	Configuring storage pools .....	105
<b>Chapter 7</b>	<b>Configuring data integrity with I/O fencing .....</b>	<b>110</b>
	About I/O fencing .....	110
	Configuring disk-based I/O fencing .....	111
	Replacing an existing coordinator disk .....	113
	Disabling I/O fencing .....	114

	Destroying the coordinator pool .....	115
	Using majority-based fencing .....	115
<b>Chapter 8</b>	<b>Configuring iSCSI disks as shared storage .....</b>	<b>117</b>
	About iSCSI .....	117
	Configuring the iSCSI initiator .....	118
	Configuring the iSCSI initiator name .....	118
	Configuring the iSCSI devices .....	119
	Configuring discovery on iSCSI .....	121
	Configuring the iSCSI targets .....	127
	Modifying tunables for iSCSI .....	132
<b>Chapter 9</b>	<b>Configuring the cloud gateway .....</b>	<b>138</b>
	About the cloud gateway .....	138
	Configuring the cloud gateway .....	139
<b>Section 4</b>	<b>Managing Veritas Access file sharing services .....</b>	<b>140</b>
<b>Chapter 10</b>	<b>Configuring your NFS server .....</b>	<b>141</b>
	About using NFS server with Veritas Access .....	141
	Using the kernel-based NFS server .....	142
	Using the NFS-Ganesha server .....	142
	Switching between NFS servers .....	143
	Recommended tuning for NFS-Ganesha version 3 and version 4 .....	143
	Accessing the NFS server .....	146
	Displaying and resetting NFS statistics .....	147
	Configuring Veritas Access for ID mapping for NFS version 4 .....	149
	Configuring the NFS client for ID mapping for NFS version 4 .....	150
	About authenticating NFS clients .....	151
	Setting up Kerberos authentication for NFS clients .....	151
	Adding and configuring Veritas Access to the Kerberos realm .....	152
<b>Chapter 11</b>	<b>Using Veritas Access as a CIFS server .....</b>	<b>155</b>
	About configuring Veritas Access for CIFS .....	156
	About configuring CIFS for standalone mode .....	157
	Configuring CIFS server status for standalone mode .....	158
	Changing security settings .....	161

Changing security settings after the CIFS server is stopped .....	161
About Active Directory (AD) .....	161
Configuring entries for Veritas Access DNS for authenticating to Active Directory (AD) .....	162
Joining Veritas Access to Active Directory (AD) .....	164
Verifying that Veritas Access has joined Active Directory (AD) successfully .....	166
About configuring CIFS for Active Directory (AD) domain mode .....	166
Configuring CIFS for the AD domain mode .....	167
Using multi-domain controller support in CIFS .....	170
About leaving an AD domain .....	171
Changing domain settings for AD domain mode .....	171
Removing the AD interface .....	174
About setting NTLM .....	175
Setting NTLM .....	175
About setting trusted domains .....	176
Specifying trusted domains that are allowed access to the CIFS server .....	177
Allowing trusted domains access to CIFS when setting an IDMAP backend to rid .....	178
Allowing trusted domains access to CIFS when setting an IDMAP backend to ldap .....	180
Allowing trusted domains access to CIFS when setting an IDMAP backend to hash .....	182
Allowing trusted domains access to CIFS when setting an IDMAP backend to ad .....	184
About configuring Windows Active Directory as an IDMAP backend for CIFS .....	185
Configuring the Active Directory schema with CIFS-schema extensions .....	186
Configuring the LDAP client for authentication using the CLI .....	191
Configuring the CIFS server with the LDAP backend .....	191
Setting Active Directory trusted domains .....	192
About storing account information .....	193
Storing user and group accounts .....	195
About reconfiguring the CIFS service .....	197
Reconfiguring the CIFS service .....	198
About mapping user names for CIFS/NFS sharing .....	200
About the mapuser commands .....	202
Adding, removing, or displaying the mapping between CIFS and NFS users .....	203
Automatically mapping of UNIX users from LDAP to Windows users .....	204

About managing home directories .....	204
Setting the home directory file systems .....	204
Setting up home directories .....	206
Displaying home directory usage information .....	208
Deleting home directories and disabling creation of home directories .....	209
About CIFS clustering modes .....	210
About load balancing for the normal clustering mode .....	211
About load balancing for the ctdb clustering mode .....	212
About switching the clustering mode .....	212
About migrating CIFS shares and home directories .....	216
Migrating CIFS shares and home directories from normal to ctdb clustering mode .....	218
Migrating CIFS shares and home directories from ctdb to normal clustering mode .....	220
Setting the CIFS aio_fork option .....	224
About managing local users and groups .....	224
Creating a local CIFS user .....	225
About configuring local groups .....	227
Configuring a local group .....	227
Enabling CIFS data migration .....	228
<b>Chapter 12</b>	<b>Using Veritas Access with Amazon S3 .....</b>
	<b>230</b>
About the object access service .....	230
About the file system hierarchy .....	231
About access management using S3 Access Control Lists .....	232
Limitations on using the Amazon S3 protocol .....	233
List of S3 APIs supported by Veritas Access .....	233
Object and bucket restrictions .....	234
Multipart uploading restrictions .....	234
Concurrent access restrictions .....	235
Secure Socket Layer (SSL) limitations .....	235
Managing the object access service .....	235
Managing Veritas Access S3 accounts .....	236
Creating buckets and objects .....	237
<b>Chapter 13</b>	<b>Configuring your FTP server .....</b>
	<b>239</b>
About FTP .....	239
Creating the FTP home directory .....	240
Using the FTP server commands .....	241
About FTP server options .....	242
Customizing the FTP server options .....	244

	Administering the FTP sessions .....	247
	Uploading the FTP logs .....	249
	Administering the FTP local user accounts .....	249
	About the settings for the FTP local user accounts .....	251
	Configuring settings for the FTP local user accounts .....	253
<b>Chapter 14</b>	<b>Configuring Veritas Access with OpenStack Cinder .....</b>	<b>255</b>
	About the Veritas Access integration with OpenStack Cinder .....	255
	About the Veritas Access integration with OpenStack Cinder architecture .....	257
	Configuring Veritas Access with OpenStack Cinder .....	258
	Configuring OpenStack Cinder .....	261
<b>Chapter 15</b>	<b>Configuring Veritas Access with OpenStack Manila .....</b>	<b>266</b>
	About the Veritas Access integration with OpenStack Manila .....	266
	OpenStack Manila use cases .....	268
	Configuring Veritas Access to work with OpenStack Manila .....	269
	Starting, stopping, or displaying the status of the REST server .....	271
	Setting the certificate of the REST server .....	272
	Enabling or disabling the SSL status of the REST server .....	272
	Changing the user password of the REST server .....	273
	Starting, stopping, or displaying the status of the OpenStack Manila service .....	273
	Configuring and managing storage pools for the OpenStack Manila user .....	275
	Adding the OpenStack Manila driver .....	276
	Creating a new share backend on the OpenStack controller node .....	277
	Restarting the OpenStack Manila driver on the OpenStack controller node .....	278
	Creating an OpenStack Manila share type .....	280
	Creating an OpenStack Manila file share .....	281
	Creating an OpenStack Manila share snapshot .....	284
	Creating an OpenStack Manila share from an OpenStack Manila share snapshot .....	284

<b>Chapter 16</b>	<b>Configuring Veritas Access to work with Oracle Direct NFS</b> .....	285
	About using Veritas Access with Oracle Direct NFS .....	285
	About the Oracle Direct NFS architecture .....	286
	Best practices for improving Oracle database performance .....	288
	About Oracle Direct NFS node or storage connection failures .....	289
	Configuring an Oracle Direct NFS storage pool .....	289
	Configuring an Oracle Direct NFS file system .....	291
	Configuring an Oracle Direct NFS share .....	292
<b>Section 5</b>	<b>Monitoring and troubleshooting</b> .....	294
<b>Chapter 17</b>	<b>Monitoring events and logs</b> .....	295
	About configuring event notifications .....	295
	About severity levels and filters .....	296
	Configuring an email group .....	296
	Configuring a syslog server .....	301
	Displaying events on the console .....	303
	About SNMP notifications .....	303
	Configuring an SNMP management server .....	304
	Configuring events for event reporting .....	307
	Exporting events in syslog format to a given URL .....	309
<b>Chapter 18</b>	<b>Displaying statistics</b> .....	310
	Displaying cluster or node statistics .....	310
	Displaying file system I/O statistics .....	312
<b>Chapter 19</b>	<b>Using the locally saved configuration files</b> .....	313
	About configuring the locally saved configuration files .....	313
	Configuring the locally saved configuration files .....	315
	Using the option commands .....	318
	Modifying the maximum amount of memory used for instant rollback cache objects .....	325
	Modifying the amount of time an unused inode spends on a freelist .....	326
<b>Chapter 20</b>	<b>Veritas Access tuning</b> .....	328
	File system mount-time memory usage .....	328

<b>Section 6</b>	<b>Provisioning and managing shares .....</b>	<b>333</b>
<b>Chapter 21</b>	<b>Creating and maintaining file systems .....</b>	<b>334</b>
	About creating and maintaining file systems .....	334
	About scale-out file systems .....	335
	Characteristics of a scale-out file system .....	336
	Considerations for creating a file system .....	337
	Best practices for creating file systems .....	337
	Choosing a file system layout type .....	339
	Determining the initial extent size for a file system .....	343
	About creating a tuned file system for a specific workload .....	344
	About FastResync .....	346
	Creating a file system .....	346
	Bringing the file system online or offline .....	350
	Listing all file systems and associated information .....	352
	Modifying a file system .....	353
	Adding or removing a mirror from a file system .....	353
	Adding or removing a column from a file system .....	355
	Increasing the size of a file system .....	356
	Decreasing the size of a file system .....	358
	About quotas for usage .....	360
	Enabling, disabling, and displaying the status of file system quotas .....	361
	Setting and displaying file system quotas .....	363
	Setting user quotas for users of specified groups .....	367
	About quotas for CIFS home directories .....	368
	Managing a file system .....	379
	Defragmenting a file system .....	379
	Checking and repairing a file system .....	384
	Configuring FastResync for a file system .....	385
	Disabling the FastResync option for a file system .....	386
	Checking and resynchronizing stale mirrors .....	387
	Setting file system alerts .....	389
	Displaying file system alert values .....	392
	Removing file system alerts .....	392
	Destroying a file system .....	393
	Upgrading disk layout versions .....	394
<b>Chapter 22</b>	<b>Creating shares for applications .....</b>	<b>398</b>
	About file sharing protocols .....	398
	About concurrent access .....	399

	Sharing directories using CIFS and NFS protocols .....	400
	Sharing a file system as a CIFS home directory .....	403
	About concurrent access with NFS and S3 .....	403
<b>Chapter 23</b>	<b>Creating and maintaining NFS shares .....</b>	<b>404</b>
	About NFS file sharing .....	404
	Displaying file systems and snapshots that can be exported .....	405
	Exporting an NFS share .....	405
	Exporting an NFS share for Kerberos authentication .....	410
	Mounting an NFS share from the NFS client .....	411
	Displaying exported directories .....	413
	About managing NFS shares using netgroups .....	414
	Configuring netgroups .....	414
	Exporting an NFS snapshot .....	417
	Unexporting a directory or deleting NFS options .....	417
<b>Chapter 24</b>	<b>Creating and maintaining CIFS shares .....</b>	<b>420</b>
	About managing CIFS shares .....	421
	Exporting a directory as a CIFS share .....	421
	Configuring a CIFS share as secondary storage for an Enterprise Vault store .....	422
	Exporting the same file system/directory as a different CIFS share .....	423
	About the CIFS export options .....	424
	Setting share properties .....	428
	Hiding system files when adding a CIFS normal share .....	429
	Displaying CIFS share properties .....	431
	Allowing specified users and groups access to the CIFS share .....	432
	Denying specified users and groups access to the CIFS share .....	433
	Exporting a CIFS snapshot .....	434
	Deleting a CIFS share .....	434
	Modifying a CIFS share .....	435
	Making a CIFS share shadow copy aware .....	436
<b>Chapter 25</b>	<b>Creating and maintaining S3 shares .....</b>	<b>438</b>
	Managing the Veritas Access S3 share .....	438

<b>Section 7</b>	<b>Managing storage services</b> .....	440
<b>Chapter 26</b>	<b>Deduplicating data</b> .....	441
	About data deduplication .....	441
	Best practices for using the Veritas Access deduplication feature .....	444
	Setting up deduplication .....	445
	Configuring deduplication .....	446
	Manually running deduplication .....	451
	Scheduling deduplication .....	453
	Setting deduplication parameters .....	456
	Removing deduplication .....	458
	Verifying deduplication .....	459
<b>Chapter 27</b>	<b>Compressing files</b> .....	462
	About compressing files .....	462
	About the compressed file format .....	463
	About the file compression attributes .....	463
	About the file compression block size .....	464
	Use cases for compressing files .....	464
	Best practices for using compression .....	464
	Compression tasks .....	464
	Compressing files .....	465
	Scheduling compression jobs .....	466
	Listing compressed files .....	469
	Showing the scheduled compression job .....	470
	Uncompressing files .....	470
	Modifying the scheduled compression .....	471
	Removing the specified schedule .....	473
	Stopping the schedule for a file system .....	473
	Removing the pattern-related rule for a file system .....	473
	Removing the modified age related rule for a file system .....	474
<b>Chapter 28</b>	<b>Configuring Veritas Access SmartTier</b> .....	475
	About Veritas Access SmartTier .....	476
	How Veritas Access uses SmartTier .....	477
	Adding tiers to a file system .....	478
	Adding or removing a column from a secondary tier of a file system .....	480
	Configuring a mirror to a tier of a file system .....	481
	Listing all of the files on the specified tier .....	483
	Displaying a list of SmartTier file systems .....	484

	Displaying the tier location of a specified file .....	484
	About tiering policies .....	484
	About configuring the policy of each tiered file system .....	485
	Configuring the policy of each tiered file system .....	486
	Best practices for setting relocation policies .....	489
	Relocating a file or directory of a tiered file system .....	490
	About configuring schedules for all tiered file systems .....	491
	Configuring schedules for tiered file systems .....	491
	Displaying the files that may be moved or pruned by running a policy .....	493
	Allowing metadata information on the file system to be written on the secondary tier .....	494
	Restricting metadata information to the primary tier only .....	495
	Removing a tier from a file system .....	495
<b>Chapter 29</b>	<b>Configuring cloud as a tier .....</b>	<b>497</b>
	Configuring the cloud as a tier feature for scale-out file systems .....	497
	Moving files between tiers in a scale-out file system .....	498
	About policies for scale-out file systems .....	502
	About pattern matching for data movement policies .....	503
	About schedules for running policies .....	504
	Creating and scheduling a policy for a scale-out file system .....	505
	Obtaining statistics on data usage in the cloud tier in scale-out file systems .....	507
<b>Chapter 30</b>	<b>Configuring SmartIO .....</b>	<b>509</b>
	About SmartIO for solid-state drives .....	509
	About SmartIO read caching for applications running on Veritas Access file systems .....	510
	Setting up SmartIO read caching for Veritas Access .....	511
	About SmartIO writeback caching for applications running on Veritas Access file systems .....	512
	Setting up SmartIO writeback caching for VxFS file systems .....	513
	Customizing the caching behavior .....	514
	Tuning the writeback caching .....	516
	Verifying the VxFS cache area and monitoring the caching .....	517
	Viewing the caching statistics for a cache area .....	518
	Flushing dirty data from a writeback cache area .....	519
	Setting the caching mode .....	520

<b>Chapter 31</b>	<b>Setting up Veritas Access Replication between two clusters</b> .....	<b>521</b>
	About Veritas Access file-level replication .....	522
	How Veritas Access Replication works .....	523
	Accessing the Veritas Access Replication commands .....	523
	Starting Veritas Access Replication .....	524
	Setting up communication between the source and the destination clusters .....	528
	Managing bandwidth limits for Veritas Access replication .....	538
	Setting up the file systems to replicate .....	541
	Setting up files to exclude from a replication unit .....	546
	Scheduling the replication .....	551
	Defining what to replicate .....	553
	About the maximum number of parallel replication jobs .....	557
	Managing a replication job .....	557
	Replicating compressed data .....	565
	Displaying replication job information and status .....	565
	Synchronizing a replication job .....	567
	Behavior of the file systems on the replication destination target .....	568
	Accessing file systems configured as replication destinations .....	568
	Creating a recovery point objective (RPO) report .....	569
	Replication job failover and failback .....	570
	Process summary .....	571
	Overview of the planned failover process .....	571
	Overview of the planned failback process .....	572
	Overview of the unplanned failover process .....	573
	Overview of the unplanned failback process .....	573
<b>Chapter 32</b>	<b>Using snapshots</b> .....	<b>574</b>
	About snapshots .....	574
	Creating snapshots .....	575
	Displaying snapshots .....	576
	Managing disk space used by snapshots .....	578
	Bringing snapshots online or taking snapshots offline .....	580
	Restoring a snapshot .....	581
	About snapshot schedules .....	582
	Configuring snapshot schedules .....	583
	Managing automated snapshots .....	586

<b>Chapter 33</b>	<b>Using instant rollbacks</b> .....	588
	About instant rollbacks .....	588
	Creating a space-optimized rollback .....	590
	Creating a full-sized rollback .....	591
	Listing Veritas Access instant rollbacks .....	592
	Restoring a file system from an instant rollback .....	592
	Refreshing an instant rollback from a file system .....	593
	Bringing an instant rollback online .....	594
	Taking an instant rollback offline .....	594
	Destroying an instant rollback .....	594
	Creating a shared cache object for Veritas Access instant rollbacks .....	595
	Listing cache objects .....	597
	Destroying a cache object of a Veritas Access instant rollback .....	599
<b>Chapter 34</b>	<b>Configuring NetBackup with Veritas Access</b> .....	600
	About the NetBackup integration with Veritas Access .....	600
	Prerequisites for configuring NetBackup .....	601
	Configuring Veritas Access for NetBackup .....	602
	Registering a NetBackup master server, an EMM server, or adding an optional media server .....	603
	Displaying the status of NetBackup services .....	604
	Configuring DNS in Veritas Access .....	606
	Configuring or changing the virtual IP address used by NetBackup .....	606
	Configuring the virtual name of NetBackup .....	607
	Adding or deleting patterns to the list of files in backups .....	607
	Displaying the included and excluded files for backups .....	608
	Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client .....	609
	Performing a backup or restore of a snapshot .....	610
	Installing or uninstalling the NetBackup client .....	610
<b>Section 8</b>	<b>Reference</b> .....	614
<b>Appendix A</b>	<b>Veritas Access documentation</b> .....	615
	Using the Veritas Access product documentation .....	615
	About accessing the online man pages .....	616
<b>Index</b> .....		618

# Introducing Veritas Access

- [Chapter 1. Introducing Veritas Access](#)
- [Chapter 2. Getting started with the Veritas Access command-line interface](#)

# Introducing Veritas Access

This chapter includes the following topics:

- [About Veritas Access](#)

## About Veritas Access

Veritas Access is a software-defined scale-out network-attached storage (NAS) solution for unstructured data that works on commodity hardware. Veritas Access provides resiliency, multi-protocol access, and data movement to and from the public cloud based on policies.

[Table 1-1](#) describes the features of Veritas Access.

**Table 1-1** Veritas Access key features

Feature	Description
Simple administration through a CLI or a GUI interface	CLI interface that provides a single point of administration for the entire cluster. GUI interface that provides a centralized dashboard with operations for creating file systems, shares, and storage pools.

**Table 1-1** Veritas Access key features (*continued*)

Feature	Description
Multi-protocol access	<p>Veritas Access includes support for the following protocols:</p> <ul style="list-style-type: none"> <li>■ Amazon S3 See <a href="#">“About the object access service”</a> on page 230.</li> <li>■ CIFS See <a href="#">“About configuring Veritas Access for CIFS”</a> on page 156.</li> <li>■ FTP See <a href="#">“About FTP”</a> on page 239.</li> <li>■ NFS See <a href="#">“About using NFS server with Veritas Access”</a> on page 141.</li> <li>■ Oracle Direct NFS See <a href="#">“About using Veritas Access with Oracle Direct NFS”</a> on page 285.</li> <li>■ SMB 3 See <a href="#">“About the CIFS export options”</a> on page 424.</li> </ul>
Flexible Storage Sharing (FSS)	<p>Enables cluster-wide network sharing of local storage.</p> <p>See <a href="#">“About Flexible Storage Sharing”</a> on page 94.</p>
Scale-out file system	<p>The following functionality is provided for a scale-out file system:</p> <ul style="list-style-type: none"> <li>■ 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. See <a href="#">“About scale-out file systems”</a> on page 335.</li> <li>■ Highly available NFS shares. See <a href="#">“Using the NFS-Ganesha server”</a> on page 142.</li> </ul>
Cloud as a tier for a scale-out file system	<p>Veritas Access supports adding a cloud service as a storage tier for a scale-out file system. You can move data between the tiers based on file name patterns and when the files were last accessed or modified. Use scheduled policies to move data between the tiers on a regular basis.</p> <p>See <a href="#">“Configuring the cloud as a tier feature for scale-out file systems”</a> on page 497.</p>
SmartIO	<p>Veritas Access supports read caching on solid state drives (SSDs) for applications running on Veritas Access file systems.</p> <p>See <a href="#">“About SmartIO for solid-state drives ”</a> on page 509.</p>

**Table 1-1** Veritas Access key features (*continued*)

Feature	Description
SmartTier	<p>Veritas Access's built-in SmartTier feature can reduce the cost of storage by moving data to lower-cost storage. Veritas Access storage tiering also facilitates the moving of data between different drive architectures.</p> <p>See <a href="#">"About Veritas Access SmartTier"</a> on page 476.</p>
Replication	<p>Periodic replication of data over IP networks.</p> <p>See <a href="#">"About Veritas Access file-level replication"</a> on page 522.</p>
Snapshot	<p>Veritas Access supports snapshots for recovering from data corruption. If files, or an entire file system, are deleted or become corrupted, you can replace them from the latest uncorrupted snapshot.</p> <p>See <a href="#">"About snapshots"</a> on page 574.</p>
Deduplication	<p>You can run post-process periodic deduplication in a file system, which eliminates duplicate data without any continuous cost.</p> <p>See <a href="#">"About data deduplication"</a> on page 441.</p>
Compression	<p>You can compress files to reduce the space used, while retaining the accessibility of the files and having the compression be transparent to applications. Compressed files look and behave almost exactly like uncompressed files: the compressed files have the same name, and can be read and written as with uncompressed files.</p> <p>See <a href="#">"About compressing files"</a> on page 462.</p>
NetBackup integration	<p>Built-in NetBackup client for backing up your file systems to a NetBackup master or media server. Once data is backed up, a storage administrator can delete unwanted data from Veritas Access to free up expensive primary storage for more data.</p> <p>See <a href="#">"About the NetBackup integration with Veritas Access"</a> on page 600.</p>

**Table 1-1** Veritas Access key features (*continued*)

Feature	Description
OpenStack plug-in	<p>Integration with OpenStack:</p> <ul style="list-style-type: none"><li>■ OpenStack Cinder integration that allows OpenStack instances to use the storage hosted by Veritas Access. See <a href="#">“About the Veritas Access integration with OpenStack Cinder”</a> on page 255.</li><li>■ OpenStack Manila integration that lets you share Veritas Access file systems with virtual machines on OpenStack Manila. See <a href="#">“About the Veritas Access integration with OpenStack Manila”</a> on page 266.</li></ul>
Quotas	Support for setting file system quotas, user quotas, and hard quotas.
Support for LDAP, NIS, and AD	Veritas Access uses the Lightweight Directory Access Protocol (LDAP) for user authentication. See <a href="#">“About configuring LDAP settings”</a> on page 74.
Partition Directory	<p>With support for partitioned directories, directory entries are redistributed into various hash directories. These hash directories are not visible in the name-space view of the user or operating system. For every new create, delete, or lookup, this feature performs a lookup for the respective hashed directory and performs the operation in that directory. This leaves the parent directory inode and its other hash directories unobstructed for access, which vastly improves file system performance.</p> <p>By default this feature is not enabled. See the <code>storage_fs(1)</code> manual page to enable this feature.</p>
Isolated storage pools	Enables you to create an isolated storage pool, which contains its own configuration files. An isolated storage pool protects the pool from losing the associated metadata if a disk in another storage pool fails.
Performance and tuning	<p>Workload-based tuning for the following workloads:</p> <ul style="list-style-type: none"><li>■ Media server</li><li>■ Virtual machine</li></ul> <p>See <a href="#">“About creating a tuned file system for a specific workload”</a> on page 344.</p>

# Getting started with the Veritas Access command-line interface

This chapter includes the following topics:

- [Logging on to Veritas Access](#)
- [Using the Veritas Access CLI](#)
- [Adding Master, System Administrator, and Storage Administrator users](#)
- [Displaying the command history](#)
- [Using the more command](#)
- [Getting help using the Veritas Access command-line interface](#)

# Logging on to Veritas Access

## To log on to the Veritas Access CLI

- ◆ To start using the Veritas Access CLI, log into the console. Use the IP address for the console that you set during the Veritas Access installation.

For the first log on, use the default user name `master`. The default password is `master`. You are prompted to change the password after your initial log on.

For subsequent log ons, use the user name `master` with the password that you have set. You can also create additional users to use with Veritas Access.

See [“Adding Master, System Administrator, and Storage Administrator users”](#) on page 24.

The End User License Agreement (EULA) is displayed the first time you log on to the Veritas Access CLI.

# Using the Veritas Access CLI

All of the Veritas Access CLI commands are organized in different modes depending on the operation you want to use. You can get a list with descriptions of all the available modes by typing a `?` mark at the CLI prompt, `clustername>`.

See [“Getting help using the Veritas Access command-line interface”](#) on page 30.

## To use the Veritas Access CLI

- ◆ Once you are logged on to the Veritas Access CLI with the appropriate role, `Master`, `System Admin`, or `Storage Admin`, enter the name of the mode you want to enter.

See [“Logging on to Veritas Access ”](#) on page 23.

See [“About user roles and privileges”](#) on page 27.

For example, to enter the `admin` mode, enter:

```
admin
```

You can see that you are in the `Admin>` mode because the cluster name is appended with the name of the command mode you specified.

```
clustername>.Admin
```

# Adding Master, System Administrator, and Storage Administrator users

The following administrator roles are included with Veritas Access:

- Master
- System Administrator
- Storage Administrator

See [“About user roles and privileges”](#) on page 27.

See [“About the naming requirements for adding new users”](#) on page 27.

You can add additional users with these roles. To add the different administrator roles, you must have `master` privilege.

---

**Note:** When adding a new user, you must assign a password.

---

## To add a Master user

- ◆ Enter the following:

```
Admin> user add username master
```

For example:

```
Admin> user add master2 master
Creating Master: master2
Success: User master2 created successfully
Changing password for master2.
New password:
Re-enter new password:
Password changed
```

## To add a System Administrator user

- ◆ Enter the following:

```
Admin> user add username system-admin
```

For example:

```
Admin> user add systemadmin1 system-admin
Creating System Admin: systemadmin1
Success: User systemadmin1 created successfully
```

### To add a Storage Administrator user

- ◆ Enter the following:

```
Admin> user add username storage-admin
```

For example:

```
Admin> user add storageadmin1 storage-admin
Creating Storage Admin: storageadmin1
Success: User storageadmin1 created successfully
```

### To change a user's password

- 1 Enter the following command to change the password for the current user:

```
Admin> passwd
```

You are prompted to enter your old password first. If the password matches, then you are prompted to enter the new password for the current user.

- 2 Enter the following command to change the password for a user other than the current user:

```
Admin> passwd [username]
```

You are prompted to enter your old password first. If the password matches, then you are prompted to enter the new password for the user.

### To display a list of current users

- 1 Enter the following to display the current user:

```
Admin> show [username]
```

- 2 Enter the following to display a list of all the current users:

```
Admin> show
```

For example:

```
Admin> show
List of Users
-----
master
user1
user2
```

Enter the following to display the details of the administrator with the user name

master:

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

### To delete a user from Veritas Access

- 1 Enter the following if you want to display the list of all the current users before deleting a user:

```
Admin> show
```

- 2 Enter the following to delete a user from Veritas Access:

```
Admin> user delete username
```

For example:

```
Admin> user delete user1
Deleting User: user1
Success: User user1 deleted successfully
```

## About user roles and privileges

Your privileges within Veritas Access are based on what user role (Master, System Administrator, or Storage Administrator) you have been assigned.

The following table provides an overview of the user roles within Veritas Access.

**Table 2-1** User roles within Veritas Access

User role	Description
Master	Masters are responsible for adding or deleting users, displaying users, and managing passwords. Only the Masters can add or delete other administrators.
System Administrator	System Administrators are responsible for configuring and maintaining the file system, NFS sharing, networking, clustering, setting the current date/time, and creating reports.
Storage Administrator	Storage Administrators are responsible for provisioning storage and exporting and reviewing reports.

The `support` account is reserved for Technical Support use only, and it cannot be created by administrators.

## About the naming requirements for adding new users

The following table provides the naming requirements for adding new Veritas Access users.

**Table 2-2** Naming requirements for adding new users

Guideline	Description
Starts with	Letter or an underscore ( <code>_</code> )  Must begin with an alphabetic character and the rest of the string should be from the following POSIX portable character set: ( <code>[A-Za-z_][A-Za-z0-9_-]*[A-Za-z0-9_-.\$]</code> ).
Length	Can be up to 31 characters. If user names are greater than 31 characters, you will receive the error, "Invalid user name."
Case	Veritas Access CLI commands are case-insensitive (for example, the user command is the same as the USER command). However, user-provided variables are case-sensitive (for example, the username <code>Master1</code> is not the same as the username <code>MASTER1</code> ).
Can contain	Hyphens ( <code>-</code> ) and underscores ( <code>_</code> ) are allowed.

**Table 2-2** Naming requirements for adding new users (*continued*)

Guideline	Description
Valid syntax	Valid user names include: <ul style="list-style-type: none"><li>▪ Name:</li><li>▪ a.b</li><li>▪ a_b</li><li>▪ _____-</li></ul>

See [“Adding Master, System Administrator, and Storage Administrator users”](#) on page 24.

## Displaying the command history

The `history` command displays the commands that you have executed. You can also view commands executed by another user.

In addition to the commands that users execute with the CLISH, the `history` command displays internal commands that were executed by Veritas Access.

You must be logged in to the system to view the command history.

See [“Getting help using the Veritas Access command-line interface”](#) on page 30.

### To display command history

- ◆ To display the command history, enter the following:

```
ACCESS> history [username] [number_of_lines]
```

*username* Displays the command history for a particular user.

*number\_of\_lines* Displays the number of lines of history you want to view.

For example:

```
ACCESS> history master 7
Username      : master
Privileges    : Master
Time          Status   Message                               Command
02-12-2016 11:09 Success  NFS> server status                    (server status)
02-12-2016 11:10 Success  NFS> server start                      (server start )
02-12-2016 11:19 Success  NFS> server stop                       (server stop )
02-12-2016 11:28 Success  NFS> fs show                           (show fs )
02-12-2016 15:00 SUCCESS  Disk list stats completed              (disk list )
02-12-2016 15:31 Success  Network shows success                  (show )
02-12-2016 15:49 Success  Network shows success                  (show )
ACCESS>
```

The information displayed from using the `history` command is:

Time	Displays the time stamp as MM-DD-YYYY HH:MM
Status	Displays the status of the command as Success, Error, or Warning.
Message	Displays the command description.
Command	Displays the actual commands that were executed by you or another user.

## Using the more command

The `System> more` command enables, disables, or checks the status of the `more` filter. The default setting is enable, which lets you page through the text one screen at a time.

### To modify and view the more filter setting

- ◆ To modify and view the `more` filter setting, enter the following:

```
System> more enable|disable|status
```

<code>enable</code>	Enables the more filter on all of the nodes in the cluster.
<code>disable</code>	Disables the more filter on all of the nodes in the cluster.
<code>status</code>	Displays the status of the <code>more</code> filter.

For example:

```
System> more status
```

```
Status : Enabled
```

```
System> more disable
```

```
ISA more Success V-288-748 more deactivated on console
```

```
System> more enable
```

```
ISA more Success V-288-751 more activated on console
```

## Getting help using the Veritas Access command-line interface

You can enter Veritas Access commands on the system console or from any host that can access Veritas Access through a session using Secure Shell (ssh).

Veritas Access provides the following features to help you when you enter commands on the command line:

- Auto-completion

The following keys both perform auto-completion for the current command line. If the command prefix is not unique, then the bell rings and a subsequent repeat of the key displays possible completions.

- `[enter]` - Auto-completes, syntax-checks then executes a command. If there is a syntax error, then the offending part of the command line is highlighted and explained.
- `[space]` - Auto-completes, or if the command is already resolved inserts a space.
- Command-line help

Type a question mark at the command line to display context-sensitive Help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, displays a detailed reference.

- Keyboard shortcut keys  
Move the cursor within the command line or delete text from the command line.  
[Table 2-4](#)
- Command-line manual pages  
Type `man` and the name of the command.
- Error reporting  
The ^ (caret) indicates a syntax error occurred in the preceding command statement. The location of a caret in the command statement indicates the location of the syntax error.
- Escape sequences  
Substitute the command line for a previous entry.  
[Table 2-5](#)

**Table 2-3** Conventions used in the Veritas Access online command-line man pages

Symbol	Description
(pipe)	Indicates you must choose one of elements on either side of the pipe.
[ ] (brackets)	Indicates that the element inside the brackets is optional.
{ } (braces)	Indicates that the element inside the braces is part of a group.
< >	Indicates a variable for which you need to supply a value.

**Table 2-4** Veritas Access command-line keyboard shortcut keys for deletions

Shortcut key	Description
[CTRL-C]	Delete the whole line.
[CTRL-U]	Delete up to the start of the line from the current position.
[CTRL-W]	Delete one word to the left from the current position.
[ALT-D]	Delete one word to the right from the current position.
[CTRL-D]	Delete the character to the right on the insertion point.

**Table 2-4** Veritas Access command-line keyboard shortcut keys for deletions (*continued*)

Shortcut key	Description
[CTRL-K]	Delete all the characters to the right of the insertion point.
[CTRL-T]	Swap the last two characters.
[backspace]	Delete the character to the left of the insertion point.
[Del]	Delete one character from the current position.

**Table 2-5** Escape sequences

Escape sequence	Description
!!	Substitute the last command line.
!N	Substitute the Nth command line (you can find the Nth command from using the <code>history</code> command).
!-N	Substitute the command line entered N lines before (the number is relative to the command you are entering).

---

**Note:** Most of the Veritas Access commands are executed asynchronously, so control may be returned to the command prompt before the operation is fully completed. For critical commands, you should verify the status of the command before proceeding. For example, after starting a CIFS resource, verify that the service is online.

---

# Configuring Veritas Access

- [Chapter 3. Configuring the Veritas Access network](#)
- [Chapter 4. Configuring authentication services](#)
- [Chapter 5. Configuring system information](#)

# Configuring the Veritas Access network

This chapter includes the following topics:

- [About configuring the Veritas Access network](#)
- [Displaying the network configuration and statistics](#)
- [About bonding Ethernet interfaces](#)
- [Bonding Ethernet interfaces](#)
- [Understanding private NIC bonding](#)
- [Configuring DNS settings](#)
- [About the IP addresses for the Ethernet interfaces](#)
- [About Ethernet interfaces](#)
- [Configuring IP addresses](#)
- [Configuring Veritas Access to use jumbo frames](#)
- [Displaying current Ethernet interfaces and states](#)
- [Configuring Ethernet interfaces](#)
- [Configuring VLAN interfaces](#)
- [Configuring NIC devices](#)
- [Monitoring NIC devices using IP addresses](#)
- [Swapping network interfaces](#)

- [Excluding PCI IDs from the cluster](#)
- [About configuring routing tables](#)
- [Configuring routing tables](#)

## About configuring the Veritas Access network

Veritas Access has the following types of networks:

- Private network  
The network between the nodes of the cluster itself. The private network is not accessible to Veritas Access client nodes.
- Public network  
The public network is visible to all clients. Veritas Access uses static IP address for its public interface networking. Veritas Access does not support DHCP for public network configuration

Veritas Access supports the following operations to manage the networking settings:

- create bond
- vlan
- change IP addresses
- add or remove network interfaces
- swap or interchange existing network interfaces

## Displaying the network configuration and statistics

You can use the `Network> show` command to display the current cluster configuration and related statistics of the cluster network configuration.

### To display the network configuration and statistics

- ◆ To display the cluster's network configuration and statistics, enter the following:

```
Network> show
```

```
Interface Statistics
```

```
-----
```

```
ACCESS_01
```

```
-----
```

Interfaces	MTU	Metric	RX-OK	RX-DROP	RX-ERR	RX-FRAME
lo	16436	1	13766	0	0	0
priveth0	1500	1	452390	0	0	0
priveth1	1500	1	325940	0	0	0
pubeth0	1500	1	25806318	0	0	0
pubeth1	1500	1	25755262	0	0	0

TX-OK	TX-DROP	TX-ERR	TX-CAR	Flag
13766	0	0	0	LRU
953273	0	0	0	BMR
506641	0	0	0	BMRU
152817	0	0	0	BMRU
673	0	0	0	BMRU

Routing Table

```

-----
ACCESS_01
-----

```

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
172.27.75.0	0.0.0.0	255.255.255.0	U	0	0	0	priveth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.182.96.1	0.0.0.0	UG	0	0	0	pubeth0

Column headers for the interface statistics portion of the output for `Network> show`

- Interfaces**            Name of the interface.
- MTU**                    Maximum Transmission Unit of the interface.
- Metric**                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 carriers lost.
FLAG	B: BROADCAST L: LOOPBACK M: MULTICAST R: RUNNING U: UP

Column headers for the routing table portion of the output for `Network> show`

Destination	The destination network or destination host.
Gateway	The gateway address or * if none is 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)
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.

See [“Configuring routing tables”](#) on page 68.

## About bonding Ethernet interfaces

Bonding associates a set of two or more Ethernet interfaces with one IP address. The association improves network performance on each Veritas Access cluster

node by increasing the potential bandwidth available on an IP address beyond the limits of a single Ethernet interface. Bonding also provides redundancy for higher availability.

For example, you can bond two 1-gigabit Ethernet interfaces together to provide up to 2 gigabits per second of throughput to a single IP address. Moreover, if one of the interfaces fails, communication continues using the single Ethernet interface.

When you create a bond, you need to specify a bonding mode. In addition, for the following bonding modes: `802.3ad`, `balance-rr`, `balance-xor`, `broadcast`, `balance-tlb`, and `balance-alb`, make sure that the base network interface driver is configured correctly for the bond type. For type `802.3ad`, the switch must be configured for link aggregation.

Consult your vendor-specific documentation for port aggregation and switch set up. You can use the `-s` option in the Linux `ethtool` command to check if the base driver supports the link speed retrieval option. The `balance-alb` bond mode type works only if the underlying interface network driver enables you to set a link address.

---

**Note:** An added IPv6 address may go into a TENTATIVE state while bonding Ethernet interfaces with `balance-rr`, `balance-xor`, or `broadcast` bond modes. While bonding with those modes, Veritas Access requires the switch to balance incoming traffic across the ports, and not deliver looped back packets or duplicates. To work around this issue, enable EtherChannel on your switch, or avoid using these bond modes.

---

**Table 3-1** Bonding mode

Index	Bonding mode	Fault tolerance	Load balancing	Switch setup	Ethtool/base driver support
0	<code>balance-rr</code>	yes	yes	yes	no
1	<code>active-backup</code>	yes	no	no	no
2	<code>balance-xor</code>	yes	yes	yes	no
3	<code>broadcast</code>	yes	no	yes	no
4	<code>802.3ad</code>	yes	yes	yes	yes (to retrieve speed)
5	<code>balance-tlb</code>	yes	yes	no	yes (to retrieve speed)

**Table 3-1** Bonding mode (*continued*)

Index	Bonding mode	Fault tolerance	Load balancing	Switch setup	Ethtool/base driver support
6	balance-alb	yes	yes	no	yes (to retrieve speed)

**Note:** When you create or remove a bond, SSH connections with Ethernet interfaces involved in that bond may be dropped. When the operation is complete, you must restore the SSH connections.

## Bonding Ethernet interfaces

The `Network> bond create` and `Network> bond remove` operations involve bringing down the interface first and then bringing them back up. This may cause the SSH connections that are hosted over those interfaces to terminate. Use the physical console of the client rather than SSH when performing `Network> bond create` and `Network> bond remove` operations.

### To display a bond

- ◆ To display a bond and the algorithm that is used to distribute traffic among the bonded interfaces, enter the following:

```
Network> bond show
```

In this example, *DEVICES* refers to Ethernet interfaces.

```
Network> bond show
```

```
BONDNAME  MODE          DEVICES
-----  ----          -
bond0     active-backup pubeth1 pubeth2
```

### To create a bond

- ◆ To create a bond between sets of two or more Ethernet interfaces on all Veritas Access cluster nodes, enter the following:

```
Network> bond create interfacelist mode option
```

<code>interfacelist</code>	Specifies a comma-separated list of public Ethernet interfaces to bond.
<code>mode</code>	Specifies how the bonded Ethernet interfaces divide the traffic.
<code>option</code>	Specifies a comma-separated option string.  Available only when the bond mode is 2 (balance-xor) or 4 (802.3ad)  <code>xmit_hash_policy</code> - specifies the transmit hash policy to use for slave selection in balance-xor and 802.3ad modes.

For example:

```
Network> bond create pubeth2,pubeth3 4 xmit_hash_policy=layer3+4
```

or

```
Network> bond create pubeth2,pubeth3 4 xmit_hash_policy=layer2
```

If the option is not specified correctly, you get an error.

You can specify a mode either as a number or a character string, as follows:

0	<code>balance-rr</code>	This mode provides fault tolerance and load balancing. It transmits packets in order from the first available slave through the last.
1	<code>active-backup</code>	Only one slave in the bond is active. If the active slave fails, a different slave becomes active. To avoid confusing the switch, the bond's MAC address is externally visible on only one port (network adapter).
2	<code>balance-xor</code>	Transmits based on the selected transmit hash policy.  The default policy is a simple.  This mode provides load balancing and fault tolerance.
3	<code>broadcast</code>	Transmits everything on all slave interfaces and provides fault tolerance.

4	802.3ad	Creates aggregation groups with the same speed and duplex settings. It uses all slaves in the active aggregator based on the 802.3ad specification.
5	balance-tlb	Provides channel bonding that does not require special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. The current slave receives incoming traffic. If the receiving slave fails, another slave takes over its MAC address.
6	balance-alb	Includes balance-tlb plus Receive Load Balancing (RLB) for IPV4 traffic. This mode does not require any special switch support. ARP negotiation load balances the receive.

### To remove a bond

- ◆ To remove a bond from all of the nodes in a cluster, enter the following:

```
Network> bond remove bondname
```

where *bondname* is the name of the bond configuration.

For example:

```
Network> bond remove bond0  
100% [#] Success: bond removed : bond0  
Network>
```

## Private bonding

- 1 The `Network> bond priv-create` command creates the bond for the private interfaces (priveth0 and priveth1) with mode 0 (*balance-rr*). Veritas Access supports only mode 0 for the private interfaces. To get the advantage of private network bonding, all private interfaces must be connected by a switch or a hub. The switch or hub ensures that if one of the NIC goes down, the communication continues with the other NIC. All services are brought offline before a bonded interface is created. This command has to be run using the server console.

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

- 2 The `Network> bond priv-remove` command removes the bonding of private interfaces (priveth0 and priveth1) for the cluster. All services are brought offline before a bonded interface is removed. This command has to be run using the server console.

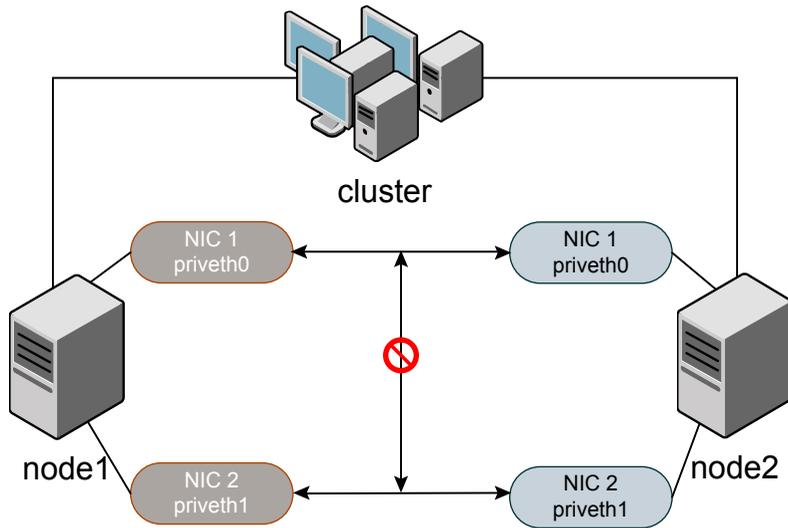
```
Network> bond priv-remove
WARNING: Removing a bond on private interfaces will OFFLINE all
services.
Do you want to continue (y/n) y
100% [#] Removing private interface bond privbond0. Please wait...
Private interfaces bond removed : privbond0
```

# Understanding private NIC bonding

This section describes how private NIC bonding works.

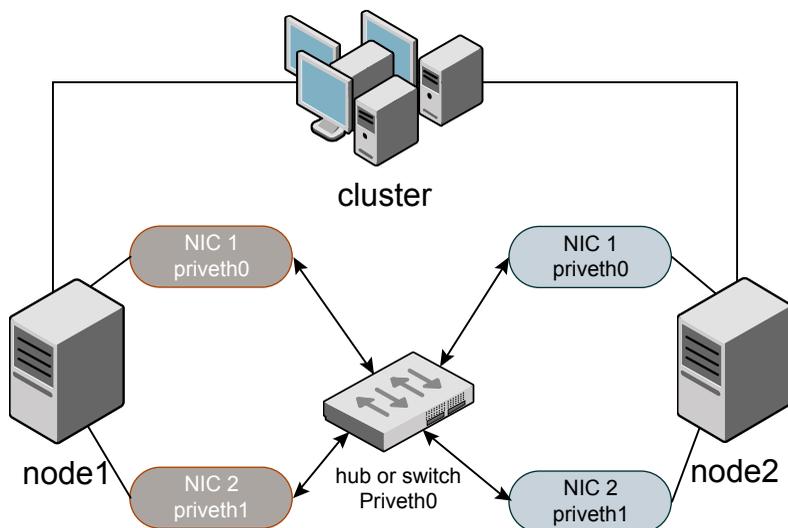
A private bond avoids single point of failure. You can upgrade or replace an individual NIC without shutting down a cluster. However, normal cluster inter-node communication relies heavily on private NICs. Once a NIC goes down, the communication efficiency slumps as one of the paths is not available.

**Figure 3-1** Private network bonding without a hub or a switch



To exploit the potential of private network bonding, it is recommended that all private interfaces should be connected by a switch or a hub. If a single NIC fails, the network communication continues with the round-robin manner. In case of double failure when two NICs on different nodes go down, the communication continues through the switch or the hub.

**Figure 3-2** Private network bonding



Note that when you create a bond with the private interfaces, there are limitations on operations such as a cluster install, cluster add, and cluster delete. The storage administrator should delete the bond before performing the operations as listed above.

## Configuring DNS settings

The Domain Name System (DNS) service resolves names to IP addresses. You can configure Veritas Access to use DNS to look up domain names and IP addresses. You enable the DNS service for the cluster, then specify up to three DNS servers.

### To display DNS settings

- ◆ To display DNS settings, enter the following:

```
Network> dns show
DNS Status      : Disabled
nameserver      : 172.16.113.118
domain          : veritas.com
```

### To enable DNS service

- ◆ To enable Veritas Access hosts to do DNS lookups and verify the results, enter the following commands:

```
Network> dns enable
Please enable/disable DNS in nsswitch settings for required services.
ACCESS dns INFO V-288-0 dns enable successful.
```

```
Network> dns show
DNS Status      : Enabled
domain          : cluster1.com
nameserver      : 10.216.50.132
```

### To disable DNS settings

- ◆ To disable DNS settings, enter the following:

```
Network> dns disable
Please enable/disable DNS in nsswitch settings for required services.
ACCESS dns INFO V-288-0 dns disable successful.
```

```
Network> dns show
DNS Status      : Disabled
Old Settings
-----
domain          : cluster1.com
nameserver      : 10.216.50.132
```

### To specify the IP addresses of the DNS name servers

- ◆ To specify the IP addresses of the DNS name servers used by the Veritas Access DNS service and verify the results, enter the following commands:

```
Network> dns set nameservers nameserver1 [nameserver2] [nameserver3]
```

For example:

```
Network> dns set nameservers 10.216.50.199 10.216.50.200
ACCESS dns INFO V-288-0 dns set nameservers successful.
```

```
Network> dns show
DNS Status      : Enabled
nameserver      : 10.216.50.199
nameserver      : 10.216.50.200
```

### To remove the name servers list used by DNS

- ◆ To remove the name servers list used by DNS and verify the results, enter the following commands:

```
Network> dns clear nameservers
ACCESS dns INFO V-288-0 dns clear nameservers successful.
```

```
Network> dns show
DNS Status      : Enabled
```

### To set the domain name for the DNS server

- ◆ To set the domain name for the DNS server, enter the following:

```
Network> dns set domainname domainname
```

where *domainname* is the domain name for the DNS server.

For example:

```
Network> dns set domainname vxindia.veritas.com  
ACCESS dns INFO V-288-0 dns set domainname successful.
```

```
Network> dns show  
DNS Status      : Enabled  
domain          : example.com  
nameserver      : 10.216.50.132
```

### To allow multiple DNS search domains

- ◆ To allow multiple DNS search domains, enter the following:

```
Network> dns set searchdomains searchdomain1[,searchdomain2]  
[,searchdomain3]
```

where *searchdomain1* is the first DNS search domain to be searched. Specify the search domains in the order in which the search domains should be used.

For example:

```
Network> dns set searchdomains 1.1.1.1,2.2.2.2,3.3.3.3  
ACCESS dns Success V-288-0 dns searchdomains successful.
```

```
Network> dns show  
DNS Status      : Enabled  
domain          : 10.200.100.170  
nameserver      : 10.198.88.18  
search          : 1.1.1.1,2.2.2.2,3.3.3.3
```

**To configure multiple DNS search domains that have already been entered**

- ◆ To configure multiple DNS search domains that have already been entered, add the existing domain name with the new domain name as comma-separated entries.

For example:

```
Network> dns show

DNS Status      : Enabled

domain          : access.com
nameserver      : 172.16.10.10
search         : domain1.access.com
```

```
Network> dns set searchdomains domain1.access.com, domain2.access.com
ACCESS dns Success V-288-2996 dns searchdomains successful.
```

```
Network> dns show

DNS Status      : Enabled

domain          : access.com
nameserver      : 172.16.10.10
search         : domain1.access.com, domain2.access.com
```

**To remove the domain name used by DNS**

- ◆ To remove the domain name used by DNS, enter the following:

```
Network> dns clear domainname
ACCESS dns INFO V-288-0 dns clear domainname successful

Network> dns show

DNS Status      : Enabled
nameserver      : 10.216.50.132
```

## About the IP addresses for the Ethernet interfaces

Internet Protocol (IP) commands configure your routing tables, Ethernet interfaces, and IP addresses, and display the settings.

The following sections describe how to configure the Ethernet interfaces:

- See [“About Ethernet interfaces”](#) on page 48.

- See “[Configuring Veritas Access to use jumbo frames](#)” on page 54.

## About Ethernet interfaces

Each Ethernet interface must have a physical IP address associated with it. These are usually supplied when the Veritas Access software is installed.

Each Ethernet interface can be configured with a virtual IP address for clustering purposes in Veritas Access. This does not imply that each interface must have a virtual IP to communicate with the network.

The physical address must be present before adding a virtual address. To add an IPv6 address on an IPv4 cluster, you have to configure the IPv6 physical address and then add the virtual address for the given interface.

## Configuring IP addresses

During installation, you specified a range of public IP addresses to be used for physical interfaces. You also specified a range for virtual interfaces. You can see which of these addresses are assigned to each node. You can use this procedure to verify the IP addresses in your configuration. You can add additional IP addresses if you want to add additional nodes and no other IP addresses are available.

### To display all the IP addresses for the cluster

- ◆ To display all of a cluster's IP addresses, enter the following:

```
Network> ip addr show
```

IP	Netmask/Prefix	Device	Node	Type	Status
--	-----	-----	----	----	-----
10.209.193.121	255.255.252.0	pubeth0	ACCESS_1	Physical	
10.209.193.122	255.255.252.0	pubeth1	ACCESS_1	Physical	
10.209.193.123	255.255.252.0	pubeth0	ACCESS_2	Physical	
10.209.193.124	255.255.252.0	pubeth1	ACCESS_2	Physical	
2001:21:0:0:0:0:2	120	pubeth0	ACCESS_1	Physical	
2001:21:0:0:0:0:3	120	pubeth0	ACCESS_2	Physical	
2001:21:0:0:0:0:4	120	pubeth1	ACCESS_1	Physical	
2001:21:0:0:0:0:5	120	pubeth1	ACCESS_2	Physical	
10.209.193.129	255.255.252.0	pubeth0	ACCESS_1	Virtual	ONLINE (Con IP)
10.209.193.125	255.255.252.0	pubeth0	ACCESS_2	Virtual	ONLINE
10.209.193.126	255.255.252.0	pubeth0	ACCESS_1	Virtual	ONLINE
10.209.193.127	255.255.252.0	pubeth1	ACCESS_2	Virtual	ONLINE
2001:21:0:0:0:0:6	120	pubeth1	ACCESS_1	Virtual	ONLINE

```
2001:21:0:0:0:0:7 120          pubeth0 ACCESS_2 Virtual ONLINE
10.209.193.128      255.255.252.0   pubeth0 ACCESS_2 Virtual ONLINE
                                                                (Replication IP)
```

The output headings are:

IP	Displays the IP addresses for the cluster.
Netmask	Displays the netmask for the IP address. Netmask is used for IPv4 addresses.  Specify an IPv4 address in the format AAA.BBB.CCC.DDD, where each number ranges from 0 to 255.
Prefix	Displays the prefix used for IPv6 addresses. The value is an integer in the range 0-128.
Device	Displays the name of the Ethernet interface for the IP address.
Node	Displays the node name associated with the interface.
Type	Displays the type of the IP address: physical or virtual.
Status	Displays the status of the IP addresses: <ul style="list-style-type: none"> <li>■ ONLINE</li> <li>■ ONLINE (console IP)</li> <li>■ OFFLINE</li> <li>■ FAULTED</li> </ul> <p>A virtual IP can be in the FAULTED state if it is already being used. It can also be in the FAULTED state if the corresponding device is not working on all nodes in the cluster (for example, a disconnected cable).</p>

### To add an IP address to a cluster

- ◆ To add an IP address to a cluster, enter the following:

```
Network> ip addr add ipaddr netmask | prefix type
[device] [nodename]
```

<code>ipaddr</code>	<p>Specifies the IP address to add to the cluster.</p> <p>Do not use physical IP addresses to access the Veritas Access cluster. In case of failure, the IP addresses cannot move between nodes. A failure could be either a node failure, an Ethernet interface failure, or a storage failure.</p> <p>You can specify either an IPv4 address or an IPv6 address.</p>
<code>netmask</code>	<p>Specifies the netmask for the IP address. Netmask is used for IPv4 addresses.</p>
<code>prefix</code>	<p>Specifies the prefix for the IPv6 address. The accepted range is 0-128 integers.</p>
<code>type</code>	<p>Specifies the IP address type, either virtual or physical.</p> <p>If <code>type</code> is <code>virtual</code>, the device is used to add new IP address on that device.</p> <p>If <code>type</code> is <code>physical</code>, the IP address gets assigned to given node on given device. In this case, you have to specify the <code>nodename</code>.</p>
<code>device</code>	<p>Only use this option if you entered <code>virtual</code> for the <code>type</code>.</p>
<code>nodename</code>	<p>Any node of the cluster</p>

For example, to add a virtual IP address on a normal device, enter the following:

```
Network> ip addr add 10.10.10.10 255.255.255.0 virtual pubeth0
ACCESS ip addr Success V-288-0 ip addr add successful.
```

For example, to add a virtual IP address on a bond device, enter the following:

```
Network> ip addr add 10.10.10.10 255.255.255.0 virtual bond0
ACCESS ip addr Success V-288-0 ip addr add successful.
```

For example, to add a virtual IPv6 address on a normal device, enter the following:

```
Network> ip addr add 2001:1::23 120 virtual pubeth0
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

For example, to add a virtual IPv6 address on any device, enter the following:

```
Network> ip addr add 2001:1::21 120 virtual
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

For example, to add a virtual IP address on a VLAN device created over a normal device with VLAN ID 3, enter the following:

```
Network> ip addr add 10.10.10.10 255.255.255.0 virtual pubeth0.3
ACCESS ip addr Success V-288-0 ip addr add successful.
```

For example, to add a virtual IP address on a VLAN device created over a bond device with VLAN ID 3, enter the following:

```
Network> ip addr add 10.10.10.10 255.255.255.0 virtual bond0.3  
ACCESS ip addr Success V-288-0 ip addr add successful.
```

For example, to add an IPv6 physical address on an interface, enter the following:

```
Network> ip addr add 2001:1::12 120 physical bond0 ACCESS_01  
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

```
Network> ip addr add 2001:21::2 120 physical pubeth0 ACCESS_01  
ACCESS ip addr WARNING V-288-227 Default gateway for IPv6 is not configured.  
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

```
Network> ip addr add 2001:21::4 120 physical pubeth1 ACCESS_01  
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

```
Network> ip addr add 22001:21::5 120 physical pubeth1 ACCESS_02  
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

```
Network> ip addr add 2001:21::6 120 virtual  
ACCESS ip addr SUCCESS V-288-1031 ip addr add successful.
```

**To change an IP address to online on a specified node**

- ◆ To change an IP address to online on a specified node, enter the following:

```
Network> ip addr online ipaddr nodename
```

**ipaddr** Specifies the IP address that needs to be brought online. You can specify either an IPv4 address or an IPv6 address.

**nodename** Specifies the nodename on which the IP address needs to be brought online. If you do not want to enter a specific nodename, enter *any* with the IP address.

For example:

```
Network> ip addr online 10.209.193.125 ACCESS_02
ACCESS ip addr SUCCESS V-288-1031 ip addr online successful.
```

```
Network> ip addr online 2001:21:0:0:0:0:0:7 ACCESS_01
ACCESS ip addr SUCCESS V-288-1031 ip addr online successful.
```

```
Network> ip addr show
```

IP	Netmask/Prefix	Device	Node	Type	Status
10.209.193.121	255.255.252.0	pubeth0	ACCESS_01	Physical	
10.209.193.122	255.255.252.0	pubeth1	ACCESS_01	Physical	
10.209.193.123	255.255.252.0	pubeth0	ACCESS_02	Physical	
10.209.193.124	255.255.252.0	pubeth1	ACCESS_02	Physical	
2001:21:0:0:0:0:0:2	120	pubeth0	ACCESS_01	Physical	
2001:21:0:0:0:0:0:3	120	pubeth0	ACCESS_02	Physical	
2001:21:0:0:0:0:0:4	120	pubeth1	ACCESS_01	Physical	
2001:21:0:0:0:0:0:5	120	pubeth1	ACCESS_02	Physical	
10.209.193.129	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE (Con IP)
10.209.193.125	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE
10.209.193.126	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE
10.209.193.127	255.255.252.0	pubeth1	ACCESS_02	Virtual	ONLINE
2001:21:0:0:0:0:0:6	120	pubeth1	ACCESS_01	Virtual	ONLINE
2001:21:0:0:0:0:0:7	120	pubeth0	ACCESS_01	Virtual	ONLINE
10.209.193.128	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE (Replication IP)

### To modify an IP address

- ◆ To modify an IP address, enter the following:

```
Network> ip addr modify oldipaddr newipaddr netmask | prefix
```

<b>oldipaddr</b>	Specifies the old IP address to be modified, as either an IPv4 address or an IPv6 address. The specified <i>oldipaddr</i> must be assigned to the cluster.
<b>newipaddr</b>	Specifies the new IP address, as either an IPv4 address or an IPv6 address. The new IP address must be available.
<b>netmask</b>	Specifies the netmask for the new IP address. Netmask is used for IPv4 addresses.
<b>prefix</b>	Specifies the prefix for the IPv6 address. The value is an integer in the range 0-128.

For example:

```
Network> ip addr modify 10.209.193.139 10.209.193.126 255.255.252.0
ACCESS ip addr Success V-288-0 ip addr modify successful.
```

```
Network> ip addr modify 2001:21:0:0:0:0:0:7 2001:21:0:0:0:0:0:8 120
ACCESS ip addr SUCCESS V-288-1031 ip addr modify successful.
```

```
Network> ip addr show
```

IP	Netmask/Prefix	Device	Node	Type	Status
10.209.193.121	255.255.252.0	pubeth0	ACCESS_01	Physical	
10.209.193.122	255.255.252.0	pubeth1	ACCESS_01	Physical	
10.209.193.123	255.255.252.0	pubeth0	ACCESS_02	Physical	
10.209.193.124	255.255.252.0	pubeth1	ACCESS_02	Physical	
2001:21:0:0:0:0:0:2	120	pubeth0	ACCESS_01	Physical	
2001:21:0:0:0:0:0:3	120	pubeth0	ACCESS_02	Physical	
2001:21:0:0:0:0:0:4	120	pubeth1	ACCESS_01	Physical	
2001:21:0:0:0:0:0:5	120	pubeth1	ACCESS_02	Physical	
10.209.193.129	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE (Con IP)
10.209.193.125	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE
10.209.193.126	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE
10.209.193.127	255.255.252.0	pubeth1	ACCESS_02	Virtual	ONLINE
2001:21:0:0:0:0:0:6	120	pubeth1	ACCESS_01	Virtual	ONLINE
2001:21:0:0:0:0:0:8	120	pubeth0	ACCESS_01	Virtual	ONLINE
10.209.193.128	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE (Replication IP)

**To remove an IP address from the cluster**

- ◆ To remove an IP address from the cluster, enter the following:

```
Network> ip addr del ipaddr
```

where *ipaddr* is either an IPv4 address or an IPv6 address.

For example:

```
Network> ip addr del 10.10.10.15
ACCESS ip addr Success V-288-0 ip addr del successful.
```

```
Network> ip addr del 2001:1::11
ACCESS ip addr SUCCESS V-288-1031 ip addr del successful.
```

```
Network> ip addr del 2001:21:0:0:0:0:8
ACCESS ip addr SUCCESS V-288-1031 ip addr del successful.
```

```
Network> ip addr show
```

IP	Netmask/Prefix	Device	Node	Type	Status
10.209.193.121	255.255.252.0	pubeth0	ACCESS_01	Physical	
10.209.193.122	255.255.252.0	pubeth1	ACCESS_01	Physical	
10.209.193.123	255.255.252.0	pubeth0	ACCESS_02	Physical	
10.209.193.124	255.255.252.0	pubeth1	ACCESS_02	Physical	
2001:21:0:0:0:0:2	120	pubeth0	ACCESS_01	Physical	
2001:21:0:0:0:0:3	120	pubeth0	ACCESS_02	Physical	
2001:21:0:0:0:0:4	120	pubeth1	ACCESS_01	Physical	
2001:21:0:0:0:0:5	120	pubeth1	ACCESS_02	Physical	
10.209.193.129	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE (Con IP)
10.209.193.125	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE
10.209.193.126	255.255.252.0	pubeth0	ACCESS_01	Virtual	ONLINE
10.209.193.127	255.255.252.0	pubeth1	ACCESS_02	Virtual	ONLINE
2001:21:0:0:0:0:6	120	pubeth1	ACCESS_01	Virtual	ONLINE
10.209.193.128	255.255.252.0	pubeth0	ACCESS_02	Virtual	ONLINE (Replication IP)

## Configuring Veritas Access to use jumbo frames

You can display and change the public Ethernet interfaces (for example, pubeth0 and pubeth1) whether a link is up or down, and the Ethernet interface's Maximum Transmission Unit (MTU) value.

The MTU value controls the maximum transmission unit size for an Ethernet frame. The standard maximum transmission unit size for Ethernet is 1500 bytes (without headers). In supported environments, the MTU value can be set to larger values up to 9000 bytes. Setting a larger frame size on an interface is commonly referred to as using jumbo frames. Jumbo frames help reduce fragmentation as data is sent over the network and in some cases, can also provide better throughput and reduced CPU usage. To take advantage of jumbo frames, the Ethernet cards, drivers, and switching must all support jumbo frames.

## Displaying current Ethernet interfaces and states

### To display current Ethernet interfaces and states

- ◆ To display current configurations, enter the following:

```
Network> ip link show [nodename][device]
```

**nodename**            Specifies which node of the cluster to display the attributes.  
                          Enter `all` to display all the IP links.

**device**             Specifies which Ethernet interface on the node to display the attributes.

```
Network> ip link show ACCESS_1 pubeth0
```

Nodename	Device	Status	MTU	Detect	Speed	HWaddr
ACCESS_01	pubeth0	UP	1500	yes	100Mb/s	00:0c:29:a8:9d:f3

To display all configurations, enter the following:

```
Network> ip link show
```

Nodename	Device	Status	MTU	Detect	Speed	HWaddr
ACCESS_01	pubeth0	UP	1500	yes	100Mb/s	00:0c:29:a8:9d:f3
ACCESS_01	pubeth1	UP	1500	yes	100Mb/s	00:0c:29:a8:9d:fd
ACCESS_02	pubeth0	UP	1500	yes	100Mb/s	00:0c:29:da:c9:e2
ACCESS_02	pubeth1	UP	1500	yes	100Mb/s	00:0c:29:da:c9:ec

# Configuring Ethernet interfaces

## To change an Ethernet interface

- ◆ To change an Ethernet interface's configuration, enter the following:

```
Network> ip link set nodename device operation [argument]
```

<b>nodename</b>	Specifies which node of the cluster to configure.  If the node specified is not part of the cluster, then an error message is displayed.  To configure all nodes at once, use the <code>all</code> option in the <code>nodename</code> field.
<b>device</b>	Specifies the Ethernet interface to configure.  If you enter an Ethernet interface that cannot be configured, an error message is displayed.
<b>operation</b>	Enter one of the following operations: <ul style="list-style-type: none"><li>■ <code>up</code> - Brings the Ethernet interface online.</li><li>■ <code>down</code> - Brings the Ethernet interface offline.</li><li>■ <code>mtu <i>MTU</i></code> - Changes the Ethernet interface's Maximum Transmission Unit (MTU) to the value that is specified in the argument field.</li></ul>
<b>argument</b>	The argument field is used only when you enter <code>mtu</code> in the operation field.  Setting the incorrect MTU value causes the console IP to become unavailable.  The argument field specifies what the MTU of the specified Ethernet interface on the specified node should be changed to.  The MTU value must be an unsigned integer between 46 and 9216.  <b>Note:</b> The acceptance of the input value is dependent on the network card driver. See your vendor-specific documentation for the valid input values.  If you enter the argument field, but do not enter an MTU in the operation field, the argument is ignored.

```
Network> ip link set all pubeth0 mtu 1600
```

```
ACCESS_01 : mtu updated on pubeth0
```

```
ACCESS_02 : mtu updated on pubeth0
```

```
Network> ip link show
```

Nodename	Device	Status	MTU	Detect	Speed	HWaddr
-----	-----	-----	---	-----	-----	-----
ACCESS_01	pubeth0	UP	1600	yes	100Mb/s	00:0c:29:a8:9d:f3
ACCESS_01	pubeth1	UP	1500	yes	100Mb/s	00:0c:29:a8:9d:fd
ACCESS_02	pubeth0	UP	1600	yes	100Mb/s	00:0c:29:da:c9:e2
ACCESS_02	pubeth1	UP	1500	yes	100Mb/s	00:0c:29:da:c9:ec

## Configuring VLAN interfaces

The virtual LAN (VLAN) feature lets you create VLAN interfaces on the Veritas Access nodes and administer them as any other VLAN interfaces. The VLAN interfaces are created using Linux support for VLAN interfaces.

Use the `Network> vlan` commands to view, add, or delete VLAN interfaces.

---

**Note:** To use VLAN, your network must have VLAN-supported switches.

---

### To display the VLAN interfaces

- ◆ To display the VLAN interfaces, enter the following:

```
Network> vlan show
```

For example:

VLAN	DEVICE	VLAN id
-----	-----	-----
pubeth0.2	pubeth0	2

**To add a VLAN interface**

- ◆ To add a VLAN interface, enter the following:

```
Network> vlan add device vlan_id
```

*device* Specifies the VLAN interface on which the VLAN interfaces will be added.

*vlan\_id* Specifies the VLAN ID which the new VLAN interface uses. Valid values range from 1 to 4095.

For example:

```
Network> vlan add pubeth1 2
```

```
Network> vlan show
```

VLAN	DEVICE	VLAN id
-----	-----	-----
pubeth0.2	pubeth0	2
pubeth1.2	pubeth1	2

**To delete a VLAN interface**

- ◆ To delete a VLAN interface, enter the following:

```
Network> vlan del vlan_device
```

where the *vlan\_device* is the VLAN name from the `Network> vlan show` command.

For example:

```
Network> vlan del pubeth0.2
```

```
Network> vlan show
```

VLAN	DEVICE	VLAN id
-----	-----	-----
pubeth1.2	pubeth1	2

# Configuring NIC devices

## To list NIC devices on a specified node

- ◆ To list NIC devices on a specified node, enter the following:

```
Network> device list nodename
```

where *nodename* is the specified node for which bus IDs and MAC addresses for all devices are listed.

For example:

```
Network> device list cls_01
Device   BusID           MAC Addr           Device Info
-----   -
priveth0 0000:02:00.0    00:50:56:be:00:9e 82545EM Gigabit Ethernet Controller (Copper)
priveth1 0000:02:01.0    00:50:56:be:00:9f 82545EM Gigabit Ethernet Controller (Copper)
pubeth0  0000:02:02.0    00:50:56:be:00:a0 82545EM Gigabit Ethernet Controller (Copper)
pubeth1  0000:02:03.0    00:50:56:be:00:a1 82545EM Gigabit Ethernet Controller (Copper)
eth1     0000:02:05.0    00:0c:29:7d:d2:8a 82545EM Gigabit Ethernet Controller (Copper)
eth2     0000:02:06.0    00:0c:29:7d:d2:94 82545EM Gigabit Ethernet Controller (Copper)
```

## To add a NIC device to a Veritas Access cluster

- ◆ To add a NIC device to a Veritas Access cluster, enter the following:

```
Network> device add devicename
```

where *devicename* is the name of the device that you want to add.

When any *eth#* device is added, the *eth#* device gets a new *pubeth#* in the Veritas Access cluster.

For example, to add a device with the name *eth2*, you would enter the following:

```
Network> device add eth2

Network> device list cls_01
Device   BusID           MAC Addr           Device Info
-----   -
priveth0 0000:02:00.0    00:50:56:be:00:9e 82545EM Gigabit Ethernet Controller (Copper)
priveth1 0000:02:01.0    00:50:56:be:00:9f 82545EM Gigabit Ethernet Controller (Copper)
pubeth0  0000:02:02.0    00:50:56:be:00:a0 82545EM Gigabit Ethernet Controller (Copper)
pubeth1  0000:02:03.0    00:50:56:be:00:a1 82545EM Gigabit Ethernet Controller (Copper)
eth1     0000:02:05.0    00:0c:29:7d:d2:8a 82545EM Gigabit Ethernet Controller (Copper)
pubeth2  0000:02:06.0    00:0c:29:7d:d2:94 82545EM Gigabit Ethernet Controller (Copper)
```

### To remove a NIC device from a Veritas Access cluster

- ◆ To remove a NIC device from a Veritas Access cluster, enter the following:

```
Network> device remove devicename
```

where *devicename* is the name of the device you want to remove.

When a device is removed, all the physical IP addresses and virtual IP addresses that are associated with the device are deleted from the specified NIC device. All physical IP addresses are kept in a free list and will be available for reuse; virtual IP addresses are not available for reuse. You need to re-add the NIC device in cases of reuse.

You can use the `Network> ip addr show` command to display the list of IP addresses associated with the device. You can see an `UNUSED` status beside the IP addresses that are free (not used).

See “[Configuring IP addresses](#)” on page 48.

For example, to remove a device `pubeth2` that is shown in the output of device list, you would enter the following:

```
Network> device remove pubeth2
```

```
Network> device list cls_01
```

Device	BusID	MAC Addr	Device Info
-----	-----	-----	-----
priveth0	0000:02:00.0	00:50:56:be:00:9e	82545EM Gigabit Ethernet Controller (Copper)
priveth1	0000:02:01.0	00:50:56:be:00:9f	82545EM Gigabit Ethernet Controller (Copper)
pubeth0	0000:02:02.0	00:50:56:be:00:a0	82545EM Gigabit Ethernet Controller (Copper)
pubeth1	0000:02:03.0	00:50:56:be:00:a1	82545EM Gigabit Ethernet Controller (Copper)
eth1	0000:02:05.0	00:0c:29:7d:d2:8a	82545EM Gigabit Ethernet Controller (Copper)
eth2	0000:02:06.0	00:0c:29:7d:d2:94	82545EM Gigabit Ethernet Controller (Copper)

### To rename a NIC device

- ◆ To rename a NIC device, enter the following:

```
Network> device rename old_name with new_name nodename
```

Only devices with the prefix `eth` can be renamed. NIC devices with new names should not be present on all nodes of the Veritas Access cluster. In cases of mismatches in names of newly-added NICs in the Veritas Access cluster, you can rename those devices, and then add the devices to the Veritas Access cluster.

For example, to rename device `eth1` with `eth0` on `cls_01`:

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

### To identify a NIC device

- ◆ To identify a NIC device, enter the following:

```
device identify devicename nodename [timeout]
```

`devicename`            Specify the name of the device you want to identify.

`nodename`             Specify the node on which the device is located.

`timeout`              By default, the timeout value is 120 seconds.

For example, to identify device `eth1` on `cls_01` with a timeout of 60 seconds, you would enter the following:

```
Network> device identify pubeth0 60
```

```
Network> 100% [#] Success: device identify successful.
```

### To replace a NIC device from a Veritas Access cluster

- 1 Delete all the VIP addresses that are related to the NIC that you want to replace using the `ippr addr del` command. Enter the following:

```
Network> ip addr del 10.193.74.182(VIP)
```

- 2 Find out the name that is related to the NIC that is to be replaced by using the `device list` command.

For example:

```
Network> device list ACCESS1S6_01
```

- 3 Remove the device from the Veritas Access configuration using the `device remove` command

For example:

```
Network> device remove pubeth3
```

- 4 Shut down the target node and replace the target NIC hardware. Then restart the system.
- 5 If new NIC name is not the same as the original device name, rename the new device name to the original device name.
- 6 Add the new NIC device.

For example:

```
Network> device add eth3
```

- 7 Add the VIP back to the device.

```
Network> ip addr add 10.193.74.182 255.255.240.0 virtual pubeth3
```

## Monitoring NIC devices using IP addresses

You can configure a set of IP addresses to monitor NIC devices. The status of the NIC device (ONLINE or OFFLINE) is dependent on whether the NIC device can ping an external IP address or not. This feature can be used only with public devices.

### To add, delete, or list the NIC devices that are used in the Veritas Access cluster

- ◆ To add monitoring IP addresses for public NIC devices, enter the following:

```
Network> device ipmonitor add devicename ipaddress1[,ipaddress2,...]
```

*devicename* Device on which the operation takes places.

*ipaddress* IP address for monitoring the NIC devices.

Use `all` to configure IP-based NIC monitoring for all public devices. A device is considered to be in working condition if it is able to ping at least one of the monitoring IP addresses.

For example:

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

### To delete IP addresses for monitoring NIC devices

- ◆ To delete IP addresses for monitoring NIC devices, enter the following:

```
Network> device ipmonitor del devicename
```

where *devicename* is the device on which the operation should take place.

Use `all` to delete IP-based NIC monitoring for all public devices.

For example:

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

### To list all the IP-based NIC monitoring IP addresses

- ◆ To list all the IP-based NIC monitoring IP addresses along with the states of the NIC devices, enter the following:

```
Network> device ipmonitor show
```

For example:

```
Network> device ipmonitor show
```

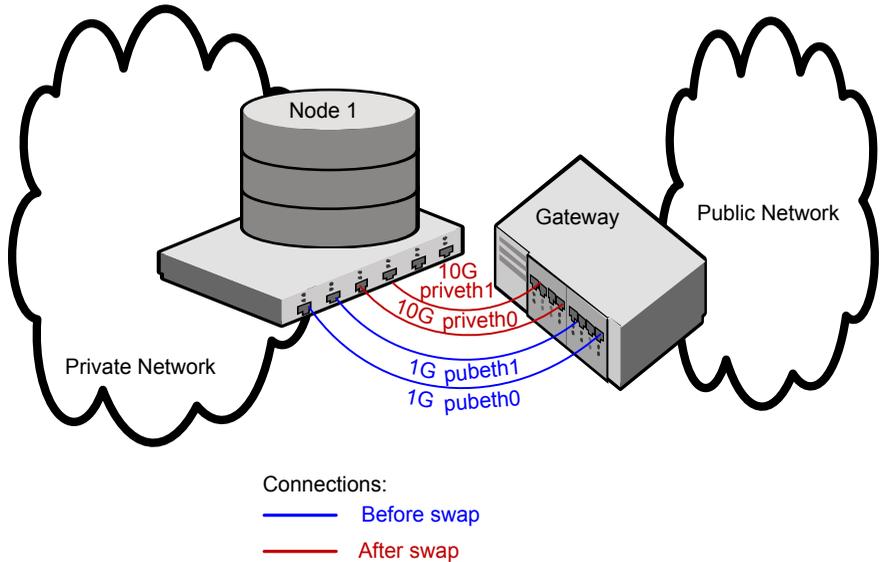
Device	Monitor IPs	dsga_01	dsga_02
pubeth0	10.29.29.29,10.29.29.30	ONLINE	ONLINE
pubeth1	10.209.107.55	ONLINE	ONLINE

## Swapping network interfaces

The `Network> swap` command can be used for swapping two network interfaces of a node in a cluster. This command helps set up the cluster properly in cases where the first node of a cluster cannot be pinged.

[Figure 3-3](#) describes a scenario whereby using the `Network> swap` command, you can use the more powerful 10G network interfaces to carry the public network load.

**Figure 3-3** Scenario for using Network> swap for network interfaces



A System Administrator can use the `Network> swap` command in the following ways:

- Multi-node cluster: You can swap one public interface with another.
- Single-node cluster: You can swap a private interface with a public interface, swap two public interfaces, or swap two private interfaces.

If input to the `Network> swap` command contains one public and one private interface, and there are two separate switches for the private and the public network, then before you run the `Network> swap` command, the System Administrator has to exchange cable connections between these interfaces.

Running the `Network> swap` command requires stopping the given interfaces, which causes the following:

- After you run the `Network> swap` command, all SSH connection(s) hosted on the input interfaces terminate.
- If a public interface is involved when issuing the `Network> swap` command, all Virtual IP addresses (VIPs) hosted on that interface are brought down first, and are brought back up after `Network> swap` is complete.
- If the `Network> swap` command is run remotely, due to SSH connection termination, its end status may not be visible to the end user. You can check

the status of the `Network> swap` command under `history`, by reconnecting to the cluster.

---

**Note:** Veritas Access recommends not to use the `Network> swap` command when active I/O load is present on the cluster.

---

### To use the swap command

- ◆ To use the `Network> swap` command, enter the following:

```
Network> swap interface1 interface2 [nodename]
```

*interface1*            Indicates the name of the first network interface.

*interface2*           Indicates the name of the second network interface.

*nodename*            Indicates the name of the node. If *nodename* is not provided, the `Network> swap` command is executed on the current node in the cluster.

For example, to swap two network interfaces:

```
Network> swap pubeth0 priveth0 ACCESS_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.
```

## Excluding PCI IDs from the cluster

During the initial Veritas Access software installation on the first node, you can exclude certain PCI IDs in your cluster to reserve them for future use. You may want to exclude additional PCI IDs when you add additional nodes to the cluster. You can add the PCI IDs to the exclusion list. The interface cards for which PCI ID's have been added in the PCI exclusion list are not used as private or public interfaces for the subsequent cluster node install. During a new node install, the remaining PCI bus interfaces are searched and added as public or private interfaces.

The `Network> pciexclusion` command can be used with different options:

- The `Network> pciexclusion show` command 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.

- The `Network> pciexclusion add pcielist` command allows an administrator to add specific PCI ID(s) for exclusion. These values must be provided before the installation. The command excludes the PCI from the second node installation.

*pcielist* is a comma-separated list of PCI IDs.

- The `Network> pciexclusion delete pci` command allows an administrator to delete a given PCI ID from exclusion. This command must be used before the installation for it to take effect. The command is effective for the next node install

The *PCI* ID bits format is hexadecimal (XXXX:XX:XX.X).

To use the `Network> pciexclusion` command, enter the following:

```
Network> pciexclusion show
```

```
PCI ID          EXCLUDED      NODENAME/UUID
-----          -
```

```
Network> pciexclusion add FFFF:FF:00.0
```

```
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has been
added for exclusion
```

```
Network> pciexclusion add FFFF:FF:00.1
```

```
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has been
added for exclusion
```

```
Network> pciexclusion show
```

```
PCI ID          EXCLUDED      NODENAME/UUID
-----          -
0000:0e:00.0 y          ACCESS_1
0000:0e:00.0 y          a79a7f43-9fe2-4eeb-aalf-27a70e7a0820
0000:04:00:1 n
```

```
Network> pciexclusion delete ffff:ff:00.1
```

```
ACCESS pciexclusion SUCCESS V-288-1363 Given PCI ID FFFF:FF:00.0 has been
added for exclusion ACCESS pciexclusion SUCCESS V-288-1364 Given PCI ID
ffff:ff:00.1 has been deleted from exclusion list
```

```
Network> pciexclusion show
```

```
PCI ID          EXCLUDED      NODENAME/UUID
-----          -
ffff:ff:00.0    n
```

```
Network>
```

## About configuring routing tables

Sometimes a Veritas Access cluster must communicate with network services (for example, LDAP) using specific gateways in the public network. In these cases, you must define routing table entries.

These entries consist of the following:

- The target network node's IP address and accompanying netmask.
- Gateway's IP address.
- Optionally, a specific Ethernet interface via which to communicate with the target. This is useful, for example, if the demands of multiple remote clients are likely to exceed a single gateway's throughput capacity.

# Configuring routing tables

## To display the routing tables of the nodes in the cluster

- ◆ To display the routing tables of the nodes in the cluster, enter the following:

```
Network> ip route show [nodename]
```

where *nodename* is the node whose routing tables you want to display. To see the routing table for all of the nodes in the cluster, enter `all`.

For example:

```
Network> ip route show all
```

```
ACCESS_01
```

```
-----
```

Destination	Gateway	Genmask	Flags	MSS	Window	irrt	Iface
172.27.75.0	0.0.0.0	255.255.255.0	U	0	0	0	priveth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.182.96.1	0.0.0.0	UG	0	0	0	pubeth0

```
ACCESS_02
```

```
-----
```

Destination	Gateway	Genmask	Flags	MSS	Window	irrt	Iface
172.27.75.0	0.0.0.0	255.255.255.0	U	0	0	0	priveth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth0
10.182.96.0	0.0.0.0	255.255.240.0	U	0	0	0	pubeth1
127.0.0.0	0.0.0.0	255.0.0.0	U	0	0	0	lo
0.0.0.0	10.182.96.1	0.0.0.0	UG	0	0	0	pubeth0

**Destination**      Displays the destination network or destination host for which the route is defined.

**Gateway**          Displays a network node equipped for interfacing with another network.

**Genmask**          Displays the netmask.

**Flags**              The flags are as follows:

U - Route is up

H - Target is a host

G - Use gateway

MSS	Displays maximum segment size. The default is 0. You cannot modify this attribute.
Window	Displays the maximum amount of data the system accepts in a single burst from the remote host. The default is 0. You cannot modify this attribute.
irtt	Displays the initial round trip time with which TCP connections start. The default is 0. You cannot modify this attribute.
iface	Displays the interface. On UNIX systems, the device name <code>lo</code> refers to the loopback interface.

### To add to the route table

- ◆ To add a route entry to the routing table of nodes in the cluster, enter the following:

```
Network> ip route add nodename ipaddr netmask
| prefix via gateway [dev device]
```

nodename	Specifies the node to whose routing table the route is to be added.  To add a route path to all the nodes, use <code>all</code> in the <i>nodename</i> field.  If you enter a node that is not a part of the cluster, an error message is displayed.
ipaddr	Specifies the destination of the IP address.  You can specify either an IPv4 address or an IPv6 address.  If you enter an invalid IP address, then a message notifies you before you fill in other fields.
netmask	Specifies the netmask associated with the IP address that is entered for the <i>ipaddr</i> field.  Use a netmask value of 255.255.255.255 for the netmask to add a host route to <i>ipaddr</i> .
prefix	Specifies the prefix for the IPv6 address. Accepted ranges are 0-128 integers.
via	This is a required field. You must type in the word.

gateway	<p>Specifies the gateway IP address used for the route.</p> <p>If you enter an invalid gateway IP address, then an error message is displayed.</p> <p>To add a route that does not use a gateway, enter a value of 0.0.0.0.</p>
dev	<p>Specifies the route device option. You must type in the word.</p>
device	<p>Specifies which Ethernet interface on the node the route path is added to. This variable is optional.</p> <p>You can specify the following values:</p> <ul style="list-style-type: none"> <li>■ any - Default</li> <li>■ pubeth0 - Public Ethernet interface</li> <li>■ pubeth1 - Public Ethernet interface</li> </ul> <p>The Ethernet interface field is required only when you specify dev in the dev field.</p> <p>If you omit the dev and device fields, Veritas Access uses a default Ethernet interface.</p>

For example:

```
Network> ip route add ACCESS_01 10.10.10.10 255.255.255.255 via 0.0.0.0 dev pubeth0
ACCESS_01: Route added successfully

Network> ip route add all :: 0 via 2001:21::1
ACCESS ip route SUCCESS V-288-369 ip route add success

Network> ip route add all 2001:21::20 128 via 2001:21::1 dev pubeth1
ACCESS ip route SUCCESS V-288-369 ip route add success
```

```
Network> ip route show
ACCESS_01
```

-----  
IPv4 routing table:

Destination	Gateway	Genmask	Flags	MSS Window	irrt	Iface
172.16.0.0	0.0.0.0	255.255.255.0	U	0 0	0	priveth0
10.209.192.0	0.0.0.0	255.255.252.0	U	0 0	0	pubeth0
10.209.192.0	0.0.0.0	255.255.252.0	U	0 0	0	pubeth1
0.0.0.0	10.209.192.1	0.0.0.0	UG	0 0	0	pubeth0

IPv6 routing table:

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
2001:21::20/128	2001:21::1	UG	1024	0	0	pubeth1
::/0	2001:21::1	UG	1024	0	0	pubeth0
2001:21::20/128	2001:21::1	UG	1024	0	0	pubeth1
2001:21::/120	::	U	1024	0	0	pubeth1
::/0	2001:21::1	UG	1024	0	0	pubeth1
2001:21::20/128	2001:21::1	UG	1024	0	0	pubeth1
2001:21::/120	::	U	256	4	0	pubeth0
2001:21::/120	::	U	256	5	0	pubeth1
fe80::/64	::	U	256	0	0	priveth0
fe80::/64	::	U	256	0	0	pubeth0
fe80::/64	::	U	256	0	0	pubeth1
::/0	2001:21::1	UG	1024	0	0	pubeth0
::1/128	::	U	0	406	3	lo
2001:21::2/128	::	U	0	49	1	lo
2001:21::4/128	::	U	0	12	1	lo
2001:21::6/128	::	U	0	0	1	lo
fe80::20c:29ff:fe88:6732/128	::	U	0	0	1	lo
fe80::20c:29ff:fe88:673c/128	::	U	0	0	1	lo
fe80::20c:29ff:fe88:6746/128	::	U	0	2	1	lo
fe80::20c:29ff:fe88:6750/128	::	U	0	3	1	lo
ff00::/8	::	U	256	0	0	priveth0
ff00::/8	::	U	256	0	0	pubeth0
ff00::/8	::	U	256	0	0	pubeth1

ACCESS\_02

-----

IPv4 routing table:

Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
172.16.0.0	0.0.0.0	255.255.255.0	U	0	0	0	priveth0
10.209.192.0	0.0.0.0	255.255.252.0	U	0	0	0	pubeth0
10.209.192.0	0.0.0.0	255.255.252.0	U	0	0	0	pubeth1
0.0.0.0	10.209.192.1	0.0.0.0	UG	0	0	0	pubeth0

IPv6 routing table:

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
2001:21::20/128	2001:21::1	UG	1024	0	0	pubeth1
::/0	2001:21::1	UG	1024	0	0	pubeth0
2001:21::20/128	2001:21::1	UG	1024	0	0	pubeth1
2001:21::/120	::	U	1024	0	0	pubeth1
::/0	2001:21::1	UG	1024	0	0	pubeth1

```

2001:21::20/128          2001:21::1          UG    1024  0      0 pubeth1
2001:21::/120           ::                  U      256   4      0 pubeth0
2001:21::/120           ::                  U      256   4      0 pubeth1
fe80::/64               ::                  U      256   0      0 priveth0
fe80::/64               ::                  U      256   0      0 pubeth0
fe80::/64               ::                  U      256   0      0 pubeth1
::1/128                 ::                  U      0     296    1 lo
2001:21::3/128          ::                  U      0     9      1 lo
2001:21::5/128          ::                  U      0     0      1 lo
fe80::20c:29ff:feb1:94ab/128 ::                  U      0     0      1 lo
fe80::20c:29ff:feb1:94b5/128 ::                  U      0     0      1 lo
fe80::20c:29ff:feb1:94bf/128 ::                  U      0     0      1 lo
fe80::20c:29ff:feb1:94c9/128 ::                  U      0     0      1 lo
ff00::/8                ::                  U      256   0      0 priveth0
ff00::/8                ::                  U      256   0      0 pubeth0
ff00::/8                ::                  U      256   0      0 pubeth1

```

**To delete route entries from the routing tables of nodes in the cluster**

- ◆ To delete route entries from the routing tables of nodes in the cluster, enter the following:

```
Network> ip route del nodename ipaddr  
          netmask | prefix
```

<code>nodename</code>	Specifies the node from which the route is deleted.  To delete the route entry from all nodes, use the <code>all</code> option in this field.
<code>ipaddr</code>	Specifies the destination IP address of the route entry to be deleted.  You can specify either an IPv4 address or an IPv6 address.  If you enter an invalid IP address, a message notifies you before you enter other fields.
<code>netmask</code>	Specifies the IP address to be used. Netmask is used for IPv4 addresses.
<code>prefix</code>	Specifies the prefix for the IPv6 address. Accepted ranges are 0-128 integers.

For example:

```
Network> ip route del ACCESS_01 10.216.128.0 255.255.255.255  
ACCESS ip route SUCCESS V-288-369 ip route del success
```

```
Network> ip route del all 2001:21::20 128  
ACCESS ip route SUCCESS V-288-369 ip route del success
```

# Configuring authentication services

This chapter includes the following topics:

- [About configuring LDAP settings](#)
- [Configuring LDAP server settings](#)
- [Administering the Veritas Access cluster's LDAP client](#)
- [Configuring the NIS-related settings](#)
- [Configuring NSS lookup order](#)

## About configuring LDAP settings

The Lightweight Directory Access Protocol (LDAP) is the protocol used to communicate with LDAP servers. The LDAP servers are the entities that perform the service. In Veritas Access, the most common use of LDAP is for user authentication.

For sites that use an LDAP server for access or authentication, Veritas Access provides a simple LDAP client configuration interface.

Before you configure Veritas Access LDAP settings, obtain the following LDAP configuration information from your system administrator:

- IP address or host name of the LDAP server. You also need the port number of the LDAP server.
- Base (or root) distinguished name (DN), for example:

```
cn=employees,c=us
```

LDAP database searches start here.

- Bind distinguished name (DN) and password, for example:

```
ou=engineering,c=us
```

This allows read access to portions of the LDAP database to search for information.

- Base DN for users, for example:

```
ou=users,dc=com
```

This allows access to the LDAP directory to search for and authenticate users.

- Base DN for groups, for example:

```
ou=groups,dc=com
```

This allows access to the LDAP database, to search for groups.

- Base DN for Netgroups, for example:

```
ou=netgroups,dc=com
```

This allows access to the LDAP database, to search for Netgroups.

- Root bind DN and password. This allows write access to the LDAP database, to modify information, such as changing a user's password.
- Secure Sockets Layer (SSL). Configures a cluster to use the Secure Sockets Layer (SSL) protocol to communicate with the LDAP server.
- Password hash algorithm, for example, `md5`, if a specific password encryption method is used with your LDAP server.

See [“Configuring LDAP server settings”](#) on page 75.

See [“Administering the Veritas Access cluster's LDAP client”](#) on page 79.

## Configuring LDAP server settings

You can set the LDAP base Distinguished Name (base DN). LDAP records are structured in a hierarchical tree. You access records through a particular path, in this case, a Distinguished Name, or DN. The base DN indicates where in the LDAP directory hierarchy you want to start your search.

---

**Note:** For Veritas Access to access an LDAP directory service, you must specify the LDAP server DNS name or IP address.

---

### To set the base DN for the LDAP server

- ◆ To set the base DN for the LDAP server, enter the following:

```
Network> ldap set basedn value
```

where *value* is the LDAP base DN in the following format:

```
dc=yourorg,dc=com
```

For example:

```
Network> ldap set basedn dc=example,dc=com
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

### To set the LDAP server hostname or IP address

- ◆ To set the LDAP server hostname or IP address, enter the following:

```
Network> ldap set server value
```

where *value* is the LDAP server hostname or IP address.

For example:

```
Network> ldap set server ldap-server.example.com
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

For example, if you enter an IP address for the value you get the following message:

```
Network> ldap set server 10.10.10.10
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

### To set the LDAP server port number

- ◆ To set the LDAP server port number, enter the following:

```
Network> ldap set port value
```

where *value* is the LDAP server port number.

For example:

```
Network> ldap set port 555
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

**To set Veritas Access to use LDAP over SSL**

- ◆ To set Veritas Access to use LDAP over SSL, enter the following:

```
Network> ldap set ssl {on|off}
```

For example:

```
Network> ldap set ssl on
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

**To set the bind DN for the LDAP server**

- ◆ To set the bind DN for the LDAP server, enter the following:

```
Network> ldap set binddn value
```

where *value* is the LDAP bind DN in the following format:

```
cn=binduser,dc=yourorg,dc=com
```

The *value* setting is mandatory.

You are prompted to supply a password. You must use your LDAP server password.

For example:

```
Network> ldap set binddn cn
```

```
Enter password for 'cn': ***
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

### To set the root bind DN for the LDAP server

- ◆ To set the root bind DN for the LDAP server, enter the following:

```
Network> ldap set rootbinddn value
```

where *value* is the LDAP root bind DN in the following format:

```
cn=admin,dc=yourorg,dc=com
```

You are prompted to supply a password. You must use your LDAP server password.

For example:

```
Network> ldap set rootbinddn dc
Enter password for 'dc': ***
Changes would be applicable after re-enable of LDAP service.
Command successfully completed.
```

### To set the LDAP users, groups, or netgroups base DN

- ◆ To set the LDAP users, groups, or netgroups base DN, enter the following:

```
Network> ldap set users-basedn value
```

```
Network> ldap set groups-basedn value
```

```
Network> ldap set netgroups-basedn value
```

**users-basedn** Specifies the value for the users-basedn. For example:  
*value*

```
ou=users,dc=example,dc=com (default)
```

**groups-basedn** Specifies the value for the groups-basedn. For example:  
*value*

```
ou=groups,dc=example,dc=com (default)
```

**netgroups-basedn** Specifies the value for the netgroups-basedn. For example:  
*value*

```
ou=netgroups,dc=example,dc=com (default)
```

For example:

```
Network> ldap set users-basedn ou=Users,dc=example,dc=com
Changes would be applicable after re-enable of LDAP service.
Command successfully completed.
```

### To set the password hash algorithm

- ◆ To set the password hash algorithm, enter the following:

```
Network> ldap set password-hash {clear|crypt|md5}
```

For example:

```
Network> ldap set password-hash clear
```

Changes would be applicable after re-enable of LDAP service.  
Command successfully completed.

### To display the LDAP configured settings

- ◆ To display the LDAP configured settings, enter the following:

```
Network> ldap get {server|port|basedn|binddn|ssl|rootbinddn|  
users-basedn|groups-basedn|netgroups-basedn|password-hash}
```

For example:

```
Network> ldap get server
```

```
LDAP server: ldap-server.example.com
```

```
OK Completed
```

### To clear the LDAP settings

- ◆ To clear the previously configured LDAP settings, enter the following:

```
Network> ldap clear {server|port|basedn|binddn|ssl|rootbinddn|  
users-basedn|groups-basedn|netgroups-basedn|password-hash}
```

For example:

```
Network> ldap clear binddn
```

```
OK Completed
```

## Administering the Veritas Access cluster's LDAP client

You can display the Lightweight Directory Access Protocol (LDAP) client configurations. LDAP clients use the LDAPv3 protocol to communicate with the server.

### To display the LDAP client configuration

- ◆ To display the LDAP client configuration, enter the following:

```
Network> ldap show [users|groups|netgroups]
```

users	Displays the LDAP users that are available in the Name Service Switch (NSS) database.
groups	Displays the LDAP groups that are available in the NSS database.
netgroups	Displays the LDAP netgroups that are available in the NSS database.

If you do not include one of the optional variables, the command displays all the configured settings for the LDAP client. For example:

```
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
```

### To enable the LDAP client configuration

- ◆ To enable the LDAP client configuration, enter the following:

```
Network> ldap enable
```

LDAP clients use the LDAPv3 protocol for communicating with the server. Enabling the LDAP client configures the Pluggable Authentication Module (PAM) files to use LDAP. PAM is the standard authentication framework for Linux.

### To disable the LDAP client configuration

- ◆ To disable the LDAP client configuration, enter the following:

```
Network> ldap disable
```

LDAP clients use the LDAPv3 protocol for communicating with the server. This command configures the PAM configuration files so that they do not use LDAP.

## Configuring the NIS-related settings

Veritas Access supports Network Information Service (NIS), implemented in a NIS server, as an authentication authority. You can use NIS to authenticate computers.

If your environment uses NIS, enable the NIS-based authentication on the Veritas Access cluster.

---

**Note:** IPv6 addresses are not supported for NIS.

---

### To display NIS-related settings

- ◆ To display NIS-related settings, enter the following:

```
Network> nis show [users|groups|netgroups]
```

users	Displays the NIS users that are available in the Veritas Access cluster's NIS database.
groups	Displays the NIS groups that are available in the Veritas Access cluster's NIS database.
netgroups	Displays the NIS netgroups that are available in the Veritas Access cluster's NIS database.

For example:

```
Network> nis show
NIS Status      : Disabled
domain         :
NIS Server     :
```

**To set the NIS domain name on all nodes in the cluster**

- ◆ To set the NIS domain name on the cluster nodes, enter the following:

```
Network> nis set domainname [domainname]
```

where *domainname* is the domain name.

For example:

```
Network> nis domainname domain_1
Setting domainname: "domain_1"
```

**To set NIS server name on all nodes in the cluster**

- ◆ To set the NIS server name on all cluster nodes, enter the following:

```
Network> nis set servername servername
```

where *servername* is the NIS server name. You can use the server's name or IP address.

For example:

```
Network> nis servername 10.10.10.10
Setting NIS Server "10.10.10.10"
```

**To enable NIS clients**

- ◆ To enable NIS clients, enter the following:

```
Network> nis enable
```

For example:

```
Network> nis enable
Enabling NIS Client on all the nodes.....
Done. Please enable NIS in nsswitch settings for required services.
```

To view the new settings, enter the following:

```
Network> nis show
NIS Status      : Enabled
domain         : domain_1
NIS Server      : 10.10.10.10
```

### To disable NIS clients

- ◆ To disable NIS clients, enter the following:

```
Network> nis disable
```

For example:

```
Network> nis disable
Disabling NIS Client on all nodes
Please disable NIS in nsswitch settings for required services.
```

## Configuring NSS lookup order

Name Service Switch (NSS) is a Veritas Access cluster service that provides a single configuration location to identify the services (such as NIS or LDAP) for network information such as hosts, groups, netgroups, passwords, and shadow files.

For example, host information may be on an NIS server. Group information may be in an LDAP database.

The NSS configuration specifies which network services the Veritas Access cluster should use to authenticate hosts, users, groups, and netgroups. The configuration also specifies the order in which multiple services should be queried.

### To display the current value set on NSS for all groups, hosts, netgroups, passwd, and shadow files

- ◆ To display the current value set on nsswitch for all groups, hosts, netgroups, passwd, and shadow files

```
Network> nsswitch show
group:   files   nis   winbind   ldap
hosts:   files   nis   dns
netgroup: files   nis
passwd:  files   nis   winbind   ldap
shadow:  files   nis   winbind
```

### To change the order of group items

- ◆ To configure the NSS lookup order, enter the following:

```
Network> nsswitch conf {group|hosts|netgroups|passwd|shadow}
value1 [[value2]] [[value3]] [[value4]]
```

<code>group</code>	Selects the group file.
<code>hosts</code>	Selects the hosts file.
<code>netgroups</code>	Selects the netgroups file.
<code>passwd</code>	Selects the password.
<code>shadow</code>	Selects the shadow file.
<code>value</code>	Specifies the following NSS lookup order with the following values: <ul style="list-style-type: none"> <li>■ <code>value1</code> (required) - { files/nis/winbind/ldap }</li> <li>■ <code>value2</code> (optional) - { files/nis/winbind/ldap }</li> <li>■ <code>value3</code> (optional) - { files/nis/winbind/ldap }</li> <li>■ <code>value4</code> (optional) - { files/nis/winbind/ldap }</li> </ul>

For example:

```
Network> nsswitch conf group nis files
Network> nsswitch show
group:    files    nis
hosts:    files    nis    dns
netgroup: nis     files
passwd:   files    nis    winbind    ldap
shadow:   files    nis    winbind
```

To select DNS, you must use the following command:

```
Network> nsswitch conf hosts

nsswitch conf hosts <value1> [value2] [value3]
--select hosts file

value1    : Choose the type (files) (files)
value2    : Type the type (files/nis/dns) []
value3    : Type the type (files/nis/dns) []
```

# Configuring system information

This chapter includes the following topics:

- [Coordinating cluster nodes to work with NTP servers](#)
- [Setting the system clock](#)

## Coordinating cluster nodes to work with NTP servers

You can set the Network Time Protocol (NTP) server on all of the nodes in the cluster. Veritas Access synchronizes the date on the NTP servers automatically. To synchronize the date manually, you can disable the NTP server and use the `System> ntp sync` command.

### To configure an NTP server for Veritas Access

- 1 To set the NTP server on all of the nodes in the cluster, enter the following:

```
System> ntp servername server-name
```

where *server-name* specifies the name of the servers or IP addresses you want to set.

Veritas Access supports multiple NTP servers, specified as a comma-separated list.

For example:

```
System> ntp servername ntp.veritas.com,10.182.128.180
ACCESS System INFO V-288-0 10.182.128.180 ntp.veritas.com has been
added into NTP server.
```

If one of the servers is unavailable, the command fails. You must specify the command again for the available servers.

For example:

```
System> ntp servername ntp.veritas.com,10.182.128.180,
unavailable.ntp.com
ACCESS System ERROR V-288-0 unavailable.ntp.com is not suitable
for synchronization
```

Use 127.127.1.0 as the IP address for selecting the local clock as the time source for the NTP server.

- 2 To display the NTP status and server name, enter the following:

```
System> ntp show
```

Example output:

```
System> ntp show
Status: Disabled
Server Name: 10.182.128.180
Server Name: ntp.veritas.com
```

- 3 To enable the NTP server on all of the nodes in the cluster, enter the following:

```
System> ntp enable
```

For example:

```
System> ntp enable
```

```
Enabling the NTP server. Done.
```

```
System> ntp show
```

```
Status      :      Enabled
Server Name:  10.182.128.180
Server Name:  ntp.veritas.com
```

**To synchronize the date on the NTP server on all the nodes in the cluster**

- 1** To disable the NTP server on all of the nodes in the cluster, enter the following:

```
System> ntp disable
```

For example:

```
System> ntp disable
Disabling the NTP server:..Done.
System> ntp show
Status      :      Disabled
Server Name:  10.182.128.180
Server Name:  ntp.veritas.com
```

- 2** To synchronize the date on the NTP server on all of the nodes in the cluster, enter the following:

```
System> ntp sync
```

---

**Note:** You must have disabled the NTP server before using the `System> ntp sync` command.

---

If there is no specific NTP servers follow the command, Veritas Access synchronizes the NTP servers you configured.

For example:

```
System> ntp disable
Disabling the NTP server. Done.

System> ntp sync
Date is synchronized on all node.
```

Veritas Access also supports synchronizing specific NTP servers.

For example:

```
System> ntp sync 10.182.128.180,ntp.veritas.com
Sync from ['10.182.128.180,ntp.veritas.com']...
Date is synchronized on all node.
```

## Setting the system clock

You use the System> clock commands to set or show the date and time of the system, including setting time zones and displaying the list of regions.

If an NTP server is configured, the NTP server corrects the time as required. Generally, you only need to use the System> clock commands if an NTP server is not configured.

See [“Coordinating cluster nodes to work with NTP servers”](#) on page 85.

---

**Warning:** Changing the system clock may cause timing conflicts for scheduled operations such as replication, SmartTier, and snapshot. Use caution when making a change.

---

## To set the system date and time

- 1 To display the current system date and time, enter the following:

```
System> clock show
```

For example:

```
System> clock show
Fri Feb 20 12:16:30 PST 2016
```

- 2 To set the system date and time, enter the following:

```
System> clock set time day month year
```

*time* HH:MM:SS using a 24-hour clock

Pacific Daylight Time (PDT) is the time zone used for the system.  
Greenwich Mean Time (GMT) is the time zone used for the BIOS.

*day* 1..31

*month* January, February, March, April, May, June, July, August,  
September, October, November, December

*year* YYYY

For example:

```
System> clock set 12:00:00 17 November 2016
.Done.
```

```
Fri Nov 17 12:00:00 PDT 2016
```

```
ACCESS clock WARNING V-288-0 Changing cluster time is dangerous and
may affect replication, DST, snapshot and other functionalities.
```

## To set the time zone and region for the system

- 1 To see the list of available timezones by region:

```
System> clock regions [region]
```

*region* Specifies the region for the system.

Valid values include:

- Africa
- America
- Asia
- Australia
- Canada
- Europe
- GMT-*offset* - (for example, GMT, GMT +1, GMT +2)
- Pacific
- US

For example:

```
System> clock regions US
```

The software displays the areas or timezones included in the `us` region.

```
System> clock regions US
```

```
Alaska  
Aleutian  
Arizona  
Central  
East-Indiana  
Eastern  
Hawaii  
Indiana-Starke  
Michigan  
Mountain  
Pacific  
Samoa
```

## 2 To set the time zone for the system, enter the following:

```
System> clock timezone timezone_string
```

The system sets to the time zone for that specific region.

For example:

```
System> clock timezone GMT  
Setting time zone to: GMT  
..Done.  
Thu Nov 17 20:00-00 GMT 2016
```

# Managing storage

- [Chapter 6. Configuring storage](#)
- [Chapter 7. Configuring data integrity with I/O fencing](#)
- [Chapter 8. Configuring iSCSI disks as shared storage](#)
- [Chapter 9. Configuring the cloud gateway](#)

# Configuring storage

This chapter includes the following topics:

- [About storage provisioning and management](#)
- [About Flexible Storage Sharing](#)
- [Displaying information for all disk devices associated with the nodes in a cluster](#)
- [Configuring disks](#)
- [Increasing the storage capacity of a LUN](#)
- [Formatting or reinitializing a disk](#)
- [Removing a disk](#)
- [Displaying WWN information](#)
- [Initiating host discovery of LUNs](#)
- [Importing new LUNs forcefully for new or existing pools](#)
- [Configuring storage pools](#)

## About storage provisioning and management

When you provision storage, you want to be able to assign the appropriate storage for the particular application. Veritas Access supports a variety of storage types. To help the users that provision the storage to select the appropriate storage, you classify the storage into groups called storage pools. A storage pool is a user-defined way to group the disks that have similar characteristics.

Veritas Access supports a wide variety of storage arrays, direct attached storage as well as in-server SSDs and HDDs. During the initial configuration, you add the disks to the Veritas Access nodes. For a storage array, a disk is a LUN from the

storage array. For best performance and resiliency, each LUN should be provisioned to all Veritas Access nodes. Local disks and fully shared disks have unique names, but partially shared disks across nodes may have the same name. Make sure that you do not assign LUNs from the same enclosure to different nodes partially.

Before you can provision storage to Veritas Access, the physical LUNs must be set up and zoned for use with the Veritas Access cluster. The storage array administrator normally allocates and zones the physical storage.

Veritas Access does not support thin reclamation disks.

After the disks are correctly discovered by Veritas Access, you assign the disks to storage pools. You create a file system on one or more storage pools. You can mirror across different pools. You can also create tiers on different pools, and use SmartTier to manage file system data across those tiers.

By default, all of the storage pools in Veritas Access share the same configuration. A copy of the configuration file resides on one of the disks in the configuration. To isolate configuration, an isolated storage pool must be created. Isolated storage pool contains its own configuration files, which protect the pool from losing the associated metadata if default configuration fails.

You can also use local disks that are shared over the network. Both DAS disks and SAN disks (LUNs) can be used by the same cluster, and you can have a mix of DAS and SAN disks in the same storage pool.

See [“About Flexible Storage Sharing”](#) on page 94.

## About Flexible Storage Sharing

Flexible Storage Sharing (FSS) enables network sharing of local storage, cluster wide. You can use both DAS disks and SAN disks (LUNs) in any storage pool that you define. Multiple storage pools can have DAS disks, and any storage pool can have a mix of DAS and SAN disks. FSS allows network shared storage to co-exist with physically shared storage, and file systems can be created using both types of storage.

---

**Note:** For FSS to work properly, ensure that the DAS disks in the servers are compliant with SCSI standards, which guarantees having a unique disk identifier (UDID). If you do not have unique UDIDs, you may run into unexpected behavior.

---

Use the following CLISH command to list all of the disks and their unique UDIDs. The UDID is displayed under the ID column.

```
Storage> disk list detail
Disk Pool Enclosure Array Type Size (Use%) Transport ID Serial Number
```

## Limitations of Flexible Storage Sharing

Note the following limitations for using FSS:

- SmartIO writeback caching is not supported.
- You cannot grow or shrink the file system unless all of the nodes in the cluster are online. Similarly, you cannot create a new file system, destroy a file system, or create a volume-level snapshot unless all of the nodes in the cluster are online.
- File systems with local disks support only full-sized rollbacks, not space-optimized rollbacks.

**Table 6-1** Commands not supported for FSS

Commands not supported for FSS	Description
SmartIO> fs cachemode writeback	SmartIO writeback caching is not supported.
Storage> fs addcolumn Storage> fs addmirror	You cannot change the layout for file systems that have DAS disks by adding columns or mirrors.
Storage> fs rmcolumn Storage> fs rmmirror	You cannot change the layout for file systems that have DAS disks by removing columns or mirrors.
Storage> fs setfastresync Storage> fs unsetfastresync	FastResync is always enabled for file systems that have DAS disks.
Storage> rollback create space-optimized	File systems with DAS disks support only full-sized rollbacks.

## Displaying information for all disk devices associated with the nodes in a cluster

You can display disk information for the disk devices associated with the nodes in the Veritas Access cluster. If local disks are present, the information includes entries for the local disks.

See the `storage_disk(1)` man page for the detailed examples.

The information displayed depends on the form of the command that you use. The following information is available:

Disk                      Indicates the disk name.

**Displaying information for all disk devices associated with the nodes in a cluster**

Serial Number	Indicates the serial number for the disk.
Enclosure	Indicates the type of storage enclosure.
Size	Indicates the size of the disk.
Use%	Indicates the percentage of the disk that is being used.
Transport	Indicates transport protocol values like SCSI, FC, and other values.
ID	<p>ID column consists of the following four fields. A ":" separates these fields.</p> <ul style="list-style-type: none"><li>■ VendorID - Specifies the name of the storage vendor, for example, HITACHI, IBM, EMC, and so on.</li><li>■ ProductID - Specifies the ProductID based on vendor. Each vendor manufactures different products. For example, HITACHI has HDS5700, HDS5800, and HDS9200 products. These products have ProductIDs such as DF350, DF400, and DF500.</li><li>■ TargetID - Specifies the TargetID. Each port of an array is a target. Two different arrays or two ports of the same array have different TargetIDs. TargetIDs start from 0.</li><li>■ LunID - Specifies the ID of the LUN. This should not be confused with the LUN serial number. LUN serial numbers uniquely identify a LUN in a target. Whereas a LunID uniquely identifies a LUN in an initiator group (or host group). Two LUNS in the same initiator group cannot have the same LunID. For example, if a LUN is assigned to two clusters, then the LunID of that LUN can be different in different clusters, but the serial number is the same.</li></ul>
Array Type	Indicates the type of storage array and can contain any one of the three values: Disk for JBODs, Active-Active, and Active-Passive.

**Displaying information for all disk devices associated with the nodes in a cluster****To display a list of disks and nodes**

- ◆ To display a list of disks and nodes, enter the following:

```
Storage> disk list
```

```
Disk                FSS_01    FSS_02    FSS_03
=====            =====
fss_01_disk_0      OK        OK        OK
fss_01_fiodrive20_0 OK        OK        OK
fss_02_disk_0      OK        OK        OK
fss_02_fiodrive20_0 NOT_CONN  OK        NOT_CONN
fss_03_disk_0      OK        OK        OK
fss_03_fiodrive20_0 NOT_CONN  NOT_CONN  OK
```

This form of the command displays local disk information for all nodes in the cluster.

**To display the disk information**

- ◆ To display the disk information, enter the following:

```
Storage> disk list detail
```

This form of the command displays local disk information from all the nodes in the cluster.

**To display the disk list paths**

- ◆ To display the disks multiple paths, enter the following:

```
Storage> disk list paths
```

```
Disk                Path  FSS_01                FSS_02                FSS_03
=====            =====
fss_01_disk_0      Path1 enabled, active        -                      -
fss_01_fiodrive20_0 Path1 enabled, active        -                      -
fss_02_disk_0      Path1 -                    enabled, active        -
fss_02_fiodrive20_0 Path1 -                    enabled, active        -
fss_03_disk_0      Path1 -                    -                      enabled, active
fss_03_fiodrive20_0 Path1 -                    -                      enabled, active
```

This form of the command displays local disk information from all the nodes in the cluster.

# Configuring disks

## To add a disk

- ◆ To add a new disk to an existing pool, enter the following:

```
Storage> pool adddisk pool_name disk1[,disk2,...]
```

pool\_name            Specifies the pool into which the disk should be added.

disk1,disk2,...      Specifies the disks to be added to the pool.

To add additional disks, use a comma with no spaces between.

A disk can only be added to one pool, so if the entered disk is already in a pool, an error message is displayed.

For example:

```
Storage> pool adddisk pool2 Disk_2
```

```
ACCESS pool Success V-288-0 Disk(s) Disk_2 are added to pool2  
successfully.
```

### To move disks from one pool to another

- ◆ To move a disk from one pool to another, or from an unallocated pool to an existing pool, enter the following:

```
Storage> pool mvdisk src_pool dest_pool disk1[,disk2,...]
```

**src\_pool** Specifies the source pool to move the disks from. If the specified source pool does not exist, an error message is displayed.

**dest\_pool** Specifies the destination pool to move the disks to. If the specified destination pool does not exist, a new pool is created with the specified name. The disk is moved to that pool.

**disk1,disk2,...** Specifies the disks to be moved.

To specify multiple disks to be moved, use a comma with no space in between.

If a specified disk is not part of the source pool or does not exist, an error message is displayed. If one of the disks to be moved does not exist, all of the specified disks to be moved will not be moved.

If all of the disks for the pool are moved, the pool is removed (deleted from the system), since there are no disks associated with the pool.

For example:

```
Storage> pool mvdisk p01 pool2 Disk_0
```

```
ACCESS pool Success V-288-0 Disk(s) moved successfully.
```

**To remove a disk**

- 1 To remove a disk from a pool, enter the following:

```
Storage> pool rmdisk disk1[,disk2,...]
```

where *disk1,disk2* specifies the disk(s) to be removed from the pool.

An unallocated pool is a reserved pool for holding disks that are removed from other pools.

For example:

```
Storage> pool list
```

Pool	Pool Type	List of disks
fss_pool	Normal	c_fss_01_disk_1 c_fss_02_disk_1
iso_pool	Isolated	st2540-0_0 st2540-0_1 st2540-0_2
test	Isolated	st2540-2_0

```
Storage> pool rmdisk st2540-2_0
```

```
ACCESS pool Success V-288-987 Disk(s) st2540-2_0 are removed
successfully.
```

```
Storage> pool list
```

Pool	Pool Type	List of disks
fss_pool	Normal	c_fss_01_disk_1 c_fss_02_disk_1
iso_pool	Isolated	st2540-0_0 st2540-0_1 st2540-0_2

The *st2540-2\_0* disk no longer appears in the output.

- 2 To remove additional disks, use a comma with no spaces in between.

For example:

```
Storage> pool rmdisk disk1,disk2
```

## Increasing the storage capacity of a LUN

The `Storage> disk grow` command lets you increase the storage capacity of a previously created LUN on a storage array disk.

---

**Warning:** 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.

---

### To increase the storage capacity of a LUN

- 1 Increase the storage capacity of the disk on your storage array. Contact your Storage Administrator for assistance.
- 2 Run the Veritas Access `Storage> scanbus` command to make sure that the disk is connected to the Veritas Access cluster.  
See “Initiating host discovery of LUNs ” on page 104.
- 3 To increase the storage capacity of the LUN, enter the following:

```
Storage> disk grow disk_name
```

where *disk\_name* is the name of the disk.

For example:

```
Storage> disk grow Disk_0
```

```
ACCESS disk SUCCESS V-288-0 disk grow Disk_0 completed successfully
```

## Formatting or reinitializing a disk

You can format or reinitialize a disk. If the disk does not belong to any group, the `Storage> disk format` command erases the first 100-MB space on the disk(s). You can format multiple disks at once.

If a DAS disk is formatted, it is exported to all the nodes in the cluster. DAS disks cannot be added to storage pools if they are not formatted.

### To reformat or reinitialize a disk

- ◆ To reformat or reinitialize a disk, enter the following:

```
Storage> disk format disk1
```

Where *disk1* is the disk that you want to format or reinitialize.

## Removing a disk

The `Storage> disk remove` command allows you to remove disks from a cluster. This command is helpful in situations when the disk attributes are incorrectly listed in Veritas Access.

---

**Note:** Only the disks that are not a part of a pool can be removed.

---

The `Storage> disk remove` command will not destroy the data on the disk, but it removes the disk from the system's configuration. Rebooting the cluster or running `scanbus` will bring back the disk into the system's configuration. To remove the disk permanently from the system's configuration, you should remove the disk's mapping from the array.

### To remove a disk from a cluster

- ◆ To remove a disk from a cluster, enter the following:

```
Storage> disk remove disk1[,disk2,...]
```

`disk1`                    Indicates the first disk name that you want to remove from the cluster.

`disk2`                    Indicates the second disk name that you want to remove from the cluster.

Disk names are comma-separated without any spaces between the disk names.

For example:

```
Storage> disk remove c_fss_01_disk_0,c_fss_02_disk_0,c_fss_03_disk_0,st2540-2_0
Warning: c_fss_01_disk_0 will be unexported!
Removed disk c_fss_01_disk_0 from c_fss_01
Removed disk st2540-2_0 from c_fss_01
Warning: c_fss_02_disk_0 will be unexported!
Removed disk c_fss_02_disk_0 from c_fss_02
Removed disk st2540-2_0 from c_fss_02
Warning: c_fss_03_disk_0 will be unexported!
Removed disk c_fss_03_disk_0 from c_fss_03
Removed disk st2540-2_0 from c_fss_03
Please remove the disks from array, else they will reappear after scanbus or
rebooting the machine.
```

## Displaying WWN information

The `Storage> hba` (Host Bus Adapter) command displays World Wide Name (WWN) information for all of the nodes in the cluster. If you want to find the WWN information for a particular node, specify the node name (host name).

### To display WWN information

- ◆ To display the WWN information, enter the following:

**Storage> hba [host\_name]**

where you can use the *host\_name* variable if you want to find WWN information for a particular node.

For example, to display WWN information for all the running nodes in the cluster, enter the following:

**Storage> hba**

```
Node                Host Initiator HBA WWNs
-----
democluster_01    21:00:00:1b:32:89:15:5f, 21:01:00:1b:32:a9:15:5f
democluster_02    21:00:00:1b:32:89:71:52, 21:01:00:1b:32:a9:71:52
```

There are two WWNs on each row that represent the two HBAs for each node.

For example, to display WWN information for a particular node, enter the following:

**Storage> hba democluster\_01**

```
HBA_Node_Name      WWN                State   Speed
-----
20:00:00:1b:32:89:15:5f 21:00:00:1b:32:89:15:5f offline 4_Gbit
20:01:00:1b:32:a9:15:5f 21:01:00:1b:32:a9:15:5f offline unknown
```

```
Support_Classes  Transmitted_FC_Frames  Received_FC_frames
-----
Class_3          445606                 1815671
Class_3          0                      0
```

```
Link_Failure_Count
-----
0
```

B.Storage>

```
democluster_01 21:00:00:1b:32:1e:5c:ba, 21:01:00:1b:32:3e:5c:ba
```

**HBA\_Node\_Name**            Displays the node name for the Host Bus Adapter (HBA).

**WWN**                      Displays World Wide Name (WWN) information.

**State**                    Available values include:

- online
- offline

Speed	Displays the speed per second.
Support_Classes	Displays the class value from <code>/sys/class/fc_host/\${host}/supported_classes</code> .
Transmitted_FC_Frames	Displays a value equal to the number of total transmitted serial attached SCSI frames across all protocols.
Received_FC_frames	Displays a value equal to the number of total received serial attached SCSI frames across all protocols.
Link_Failure_Count	Displays a value equal to the value of the LINK FAILURE COUNT field of the Link Error Status.

## Initiating host discovery of LUNs

The `Storage> scanbus` command scans all of the SCSI devices connected to all of the nodes in the cluster. When you add new storage to your devices, you must scan for new SCSI devices. You only need to issue the command once and all of the nodes discover the newly added disks. The `scanbus` command updates the device configurations without interrupting the existing I/O activity. The scan does not inform you if there is a change in the storage configuration. You can see the latest storage configuration using the `Storage> disk list` command.

You do not need to reboot after `scanbus` has completed.

### To scan SCSI devices

- ◆ To scan the SCSI devices connected to all of the nodes in the cluster, enter the following:

```
Storage> scanbus
```

For example:

```
Storage> scanbus
100% [#] Scanning the bus for disks
```

## Importing new LUNs forcefully for new or existing pools

The `Storage> scanbus force` command tries to import Logical Unit Numbers (LUNs) forcefully. This may help when using `Storage> scanbus` alone does not work.

**To import LUNs forcefully**

- ◆ To import LUNs forcefully, enter the following:

```
Storage> scanbus [force]
```

## Configuring storage pools

A storage pool is a group of disks that Veritas Access uses for allocation. Before creating a file system, you must create a storage pool.

## To create the storage pool used to create a file system

- 1 List all of the available disks, and identify which ones you want to assign to which pools.

```
Storage> disk list
Disk          ACCESS_01
====          =====
disk1         OK
```

- 2 To create a storage pool, enter the following:

```
Storage> pool create pool_name disk1[,disk2,...] [isolated=yes|no]
```

pool_name	Specifies what the created storage pool will be named. The storage pool name should be a string.
disk1, disk2,...	Specifies the disks to include in the storage pool. If the specified disk does not exist, an error message is displayed. Use the <code>Storage&gt; disk list</code> command to view the available disks.  Each disk can only belong to one storage pool. If you try to add a disk that is already in use, an error message is displayed.  To specify additional disks to be part of the storage pool, use a comma with no space in between.
isolated=yes no	Optional. Specifies whether or not the storage pool is isolated from other storage pools. Isolating the storage pool means that the configuration information is not shared. By default, storage pools are not isolated.

For example:

```
Storage> pool create pool1 Disk_0,Disk_1
ACCESS pool Success V-288-1015 Pool pool1 created successfully
100% [#] Creating pool pool1
```

### To list your pools

- ◆ To list your pools, enter the following:

```
Storage> pool list
```

If a node is down, the `Storage> pool list` command shows local disks of that node.

For example:

```
Storage> pool list
Pool      Pool Type  List of disks
=====  =====  =====
fss_pool  Normal    c_fss_01_disk_1 c_fss_02_disk_1
iso_pool  Isolated  st2540-0_0 st2540-0_1 st2540-0_2
test     Isolated  st2540-2_0
```

### To rename a pool

- ◆ To rename a pool, enter the following:

```
Storage> pool rename old_name new_name
```

`old_name` Specifies the name for the existing pool that will be changed. If the old name is not the name of an existing pool, an error message is displayed.

`new_name` Specifies the new name for the pool. If the specified new name for the pool is already being used by another pool, an error message is displayed.

For example:

```
Storage> pool rename pool1 p01
ACCESS pool Success V-288-0 Disk(s) Pool rename successful.
```

### To destroy a storage pool

- 1 Because you cannot destroy an `Unallocated` storage pool, you need to remove the disk from the storage pool using the `Storage> pool rmdisk` command prior to trying to destroy the storage pool.

See “Configuring disks” on page 98.

If you want to move the disk from the unallocated pool to another existing pool, you can use the `Storage> pool mvdisk` command.

See “Configuring disks” on page 98.

- 2 To destroy a storage pool, enter the following:

```
Storage> pool destroy pool_name
```

Where *pool\_name* specifies the storage pool to delete. If the specified *pool\_name* is not an existing storage pool, an error message is displayed.

If a node is down temporarily, it is not a good practice to destroy a storage pool that contains local disks of that node.

For example:

```
Storage> pool destroy pool1
```

```
ACCESS pool Success V-288-988 Pool pool1 is destroyed.
```

---

**Note:** You cannot destroy the last non-isolated pool if isolated pools exist.

---

**To list free space for pools**

- ◆ To list free space for your pool, enter the following:

```
Storage> pool free [pool_name]
```

Where *pool\_name* specifies the pool for which you want to display free space information.

If a specified pool does not exist, an error message is displayed.

If *pool\_name* is omitted, the free space for every pool is displayed, but information for specific disks is not displayed.

For example:

```
Storage> pool free
```

Pool	Free Space	Total Space	Use%
====	=====	=====	====
pool_1	0 KB	165.49M	100%
pool_2	0 KB	165.49M	100%
pool_3	57.46M	165.49M	65%

# Configuring data integrity with I/O fencing

This chapter includes the following topics:

- [About I/O fencing](#)
- [Configuring disk-based I/O fencing](#)
- [Using majority-based fencing](#)

## About I/O fencing

In the Veritas Access cluster, one method of communication between the nodes is conducted through heartbeats over private links. If the two nodes cannot communicate, the two nodes cannot verify each other's state. Neither node can distinguish if the failed communication is because of a failed link or a failed partner node. The network breaks into two networks that cannot communicate with each other but do communicate with the central storage. This condition is referred to as the "split-brain" condition.

I/O fencing protects data integrity if the split-brain condition occurs. I/O fencing determines which nodes retain access to the shared storage and which nodes are removed from the cluster, to prevent possible data corruption.

In Veritas Access, I/O fencing has the following modes:

- Disk-based I/O fencing uses coordinator disks for arbitration in the event of a network partition. Coordinator disks are standard disks or LUNs that are set aside for use by the I/O fencing driver. The coordinator disks act as a global lock device during a cluster reconfiguration. This lock mechanism determines which node is allowed to fence off data drives from other nodes. A system must eject a peer from the coordinator disks before it can fence the peer from the

data drives. Racing for control of coordinator disks is how fencing helps prevent split-brain. Coordinator disks cannot be used for any other purpose. You cannot store data on them.

To use the disk-based I/O fencing feature, you enable fencing on each node in the cluster. Disk-based I/O fencing always requires an odd number of disks starting with three disks. You must also specify the three disks to use as coordinator disks. The minimum configuration must be a two-node cluster with Veritas Access software installed and more than three disks. Three of the disks are used as coordinator disks and the rest of the disks are used for storing data. See [“Configuring disk-based I/O fencing”](#) on page 111.

- Majority-based I/O fencing provides support for high availability when there are no additional servers or shared SCSI-3 disks that can act as coordination points. The cluster must have an odd number of nodes. In case a split-brain condition occurs, the sub-cluster with more than half of the nodes remains online. If a sub-cluster has less than half of the nodes, then it panics itself. For Veritas Access, majority-based fencing is used for Flexible Storage Sharing. See [“About Flexible Storage Sharing”](#) on page 94. Majority-based I/O fencing is administered only with the CLISH. See [“Using majority-based fencing”](#) on page 115.

## Configuring disk-based I/O fencing

To use the disk-based I/O fencing feature, the minimum configuration must be a two-node cluster with Veritas Access software installed and more than three disks. Three disks are used as coordinator disks and the rest of the disks are used for storing data.

Enabling I/O fencing configures disk-based fencing if shared disks are present.

---

**Note:** Enabling I/O fencing causes a disruption of Veritas Access services. It is suggested to bring down the Veritas Access services, enable I/O fencing, and then resume Veritas Access services.

---

**To configure I/O fencing**

- 1 To check the status of I/O fencing, enter the following:

```
Storage> fencing status
```

In the following example, I/O fencing is configured on the three disks *Disk\_0*, *Disk\_1* and *Disk\_2* and the column header **Coord Flag On** indicates that these disks are in good condition. If you check the `Storage> disk list` output, it will be in the **OK** state.

```
IO Fencing Status
=====
      Disabled

Disk Name          Coord Flag On
=====          =====
Disk_0             Yes
Disk_1             Yes
Disk_2             Yes
```

- 2 If there are not three coordinator disks, you must add coordinator disks. You can add disks and enable fencing at the same time with the following command:

```
Storage> fencing on disk1,disk2,disk3
```

If at least three coordinator disks are in good condition, you can enable I/O fencing with the following command:

```
Storage> fencing on
```

For example:

```
Storage> fencing on
```

```
ACCESS fencing Success V-288-0 IO Fencing feature now Enabled  
100% [#] Enabling fencing
```

```
Storage> fencing status
```

```
IO Fencing Status
```

```
=====
```

```
Enabled
```

Disk Name	Coord Flag On
=====	=====
Disk_0	Yes
Disk_1	Yes
Disk_2	Yes

You may still provide three disks for fencing if three coordinator disks already exist. This will, however, remove the three coordinator disks previously used for fencing, and configure I/O fencing on the new disks.

## Replacing an existing coordinator disk

You can replace a coordinator disk with another disk. The replacement disk must not be in a failed state, and must not be in use by an existing pool.

---

**Note:** If the disk being replaced is in a failed state, then you must delete the disk from the array. If the failed disk comes up and works properly, it can lead to an even number of fencing disks, and this affects the functionality.

---

### To replace an existing coordinator disk

- ◆ To replace the existing coordinator disk, enter the following:

```
Storage> fencing replace src_disk dest_disk
```

where *src\_disk* is the source disk and *dest\_disk* is the destination disk.

For example:

```
Storage> fencing replace Disk_2 Disk_3
ACCESS fencing Success V-288-0 Replaced disk Disk_2
with Disk_3 successfully.
100% [#] Replacing disk Disk_2 with Disk_3
Storage> fencing status
IO Fencing Status
=====
                Enabled

Disk Name                Coord Flag On
=====                =====
Disk_0                    Yes
Disk_1                    Yes
Disk_3                    Yes
```

## Disabling I/O fencing

You can disable I/O fencing on all of the nodes. This operation does not free up the coordinator disks.

---

**Note:** Disabling I/O fencing causes a disruption of Veritas Access services. It is suggested to bring down the Veritas Access services, disable I/O fencing, and then resume Veritas Access services.

---

### To disable I/O fencing

- ◆ To disable I/O fencing, enter the following:

```
Storage> fencing off
```

For example, to disable fencing if it's already enabled:

```
Storage> fencing off
ACCESS fencing Success V-288-0 IO Fencing feature now Disabled
100% [#] Disabling fencing
```

## Destroying the coordinator pool

Destroys the coordinator pool if I/O fencing is disabled.

---

**Note:** This operation is not supported for a single-node cluster.

---

### To destroy the coordinator pool

- ◆ To destroy the coordinator pool, enter the following:

```
Storage> fencing destroy
```

## Using majority-based fencing

For Flexible Storage Sharing (FSS), you are prompted for the type of fencing (majority-based or disk-based) that you want to set. Majority-based fencing does not require configuring a coordinator pool or coordinator disks. Enabling I/O fencing configures majority-based fencing if no shared disks are present.

---

**Note:** Enabling or disabling I/O fencing causes a disruption of Veritas Access services. Veritas suggests that you bring down the Veritas Access services, enable or disable I/O fencing, and then resume Veritas Access services.

---

### To check the status of I/O fencing

- ◆ Check the status of I/O fencing while I/O fencing is not enabled.

```
Storage> fencing status
IO Fencing Status
=====
Disabled
```

## To enable majority-based fencing

- 1 Enable majority-based I/O fencing.

```
Storage> fencing on majority
```

For example:

```
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
```

- 2 Check the status of I/O fencing after enabling I/O fencing.

```
Storage> fencing status
```

```
IO Fencing Status
```

```
=====
```

```
Majority Fencing Enabled
```

## To disable majority-based I/O fencing

- ◆ Disable majority-based I/O fencing.

```
Storage> fencing off
```

For example, to disable I/O fencing if it is already enabled:

```
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
```

# Configuring iSCSI disks as shared storage

This chapter includes the following topics:

- [About iSCSI](#)
- [Configuring the iSCSI initiator](#)
- [Configuring the iSCSI initiator name](#)
- [Configuring the iSCSI devices](#)
- [Configuring discovery on iSCSI](#)
- [Configuring the iSCSI targets](#)
- [Modifying tunables for iSCSI](#)

## About iSCSI

The Internet Small Computer System Interface (iSCSI) is an Internet protocol-based storage networking standard that links data storage facilities. By carrying SCSI commands over IP networks, iSCSI facilitates data transfers over Intranets and manages storage over long distances.

The iSCSI feature allows Veritas Access servers to use iSCSI disks as shared storage. Veritas Access can just act as a iSCSI initiator and not as a iSCSI target system.

# Configuring the iSCSI initiator

## To display the iSCSI initiator service

- ◆ To display the status of the iSCSI initiator service, enter the following:

```
Storage> iscsi status
```

For example:

```
iscsi Initiator Status on ACCESS_01 : ONLINE  
iscsi Initiator Status on ACCESS_02 : ONLINE
```

## To start the iSCSI initiator service

- ◆ To start the iSCSI initiator service, enter the following:

```
Storage> iscsi start
```

For example:

```
Storage> iscsi start  
Storage> iscsi status  
iscsi Initiator Status on ACCESS_01 : ONLINE  
iscsi Initiator Status on ACCESS_02 : ONLINE
```

## To stop the iSCSI initiator service

- ◆ To stop the iSCSI initiator service, enter the following:

```
Storage> iscsi stop
```

For example:

```
Storage> iscsi stop  
Storage> iscsi status  
iscsi Initiator Status on ACCESS_01 : OFFLINE  
iscsi Initiator Status on ACCESS_02 : OFFLINE
```

# Configuring the iSCSI initiator name

Veritas Access generates iSCSI initiator names for each node.

You can set the prefix that Veritas Access uses to generate initiator names. Veritas Access names each initiator with this prefix followed by the node number of the node.

### To display the iSCSI initiator names

- ◆ To display the iSCSI initiator names, enter the following:

```
Storage> iscsi initiator name list
```

For example:

```
Storage> iscsi initiator name list
Node           Initiator Name
----           -
ACCESS_01     iqn.2009-05.com.test:test.1
ACCESS_02     iqn.2009-05.com.test:test.2
```

### To configure the iSCSI initiator name

- ◆ To configure the iSCSI initiator name prefix, enter the following:

```
Storage> iscsi initiator name setprefix initiatorname-prefix
```

where *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.

For example:

```
Storage> iscsi initiator name setprefix iqn.2009-05.com.test:test
```

## Configuring the iSCSI devices

The iSCSI initiator contains a list of network devices (network interfaces) from which connections are made to targets.

You can add or delete devices from this list.

When you 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 targets by using the newly set devices.

When you delete a `device` from the iSCSI configuration, any existing connections by way of the `device` to targets is terminated. If there are existing targets, you cannot delete the last device in the iSCSI initiator configuration.

### To display the list of devices

- ◆ To display the list of devices, enter the following:

```
Storage> iscsi device list
```

For example:

```
Storage> iscsi device list
Device
-----
pubeth0
pubeth1
```

### To add an iSCSI device

- ◆ To add an iSCSI device, enter the following:

```
Storage> iscsi device add device
```

where *device* is the device where the operation takes place.

For example:

```
Storage> iscsi device add pubeth1
Storage> iscsi device list
Device
-----
pubeth0
pubeth1
```

### To delete an iSCSI device

- ◆ To delete an iSCSI device, enter the following:

```
Storage> iscsi device delete device
```

where *device* is the device where the operation takes place.

For example:

```
Storage> iscsi device add pubeth1
Storage> iscsi device list
Device
-----
pubeth0
```

# Configuring discovery on iSCSI

The iSCSI initiator contains a list of iSCSI target discovery addresses.

## To display the iSCSI discovery addresses

- ◆ To display the iSCSI discovery addresses, enter the following:

```
Storage> iscsi discovery list
```

For example:

```
Storage> iscsi discovery list
```

```
Discovery Address
```

```
-----
```

```
192.168.2.14:3260
```

```
192.168.2.15:3260
```

## To add a discovery address to the iSCSI initiator

- 1 To add a discovery address to the iSCSI initiator, enter the following:

```
Storage> iscsi discovery add discovery-address
```

where:

***discovery-address*** The target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720.

You can specify either an IPv4 address or an IPv6 address.

Optionally, you can specify a port with the IP address. For example:

```
192.168.0.4  
192.168.0.4:3260  
2001:c90::211:9ff:feb8:a9e9  
[2001:c90::211:9ff:feb8:a9e9]:3260
```

If no port is specified, the default port 3260 is used. Verify that your firewall allows you to access the target location through the port. For example:

```
# telnet discovery-address 3260
```

For example:

```
Storage> iscsi discovery add 192.168.2.15:3260  
Discovery CHAP credentials for ACCESS_1:  
Outgoing CHAP Username : root  
Outgoing CHAP Password : *****  
Incoming CHAP Username :  
Authentication succeeded.
```

Discovered Targets

-----

```
iqn.2001-04.com.example:storage.disk2.sys3.xyz  
iqn.2001-04.com.example:storage.disk3.sys3.xyz  
iqn.2001-04.com.example:storage.disk4.sys3.xyz  
iqn.2001-04.com.example:storage.disk5.sys3.xyz
```

```
Logging into target iqn.2001-04.com.example:storage.disk2.sys3.xyz  
Logging into target iqn.2001-04.com.example:storage.disk3.sys3.xyz  
Logging into target iqn.2001-04.com.example:storage.disk4.sys3.xyz  
Logging into target iqn.2001-04.com.example:storage.disk5.sys3.xyz
```

- 2 To verify the addition of the discovery address, display the discovery addresses.

```
Storage> iscsi discovery list
```

For example:

```
Storage> iscsi discovery list
```

```
Discovery Address
```

```
-----
```

```
192.168.2.14:3260
```

```
192.168.2.15:3260
```

## To delete an iSCSI discovery address

- 1 To delete the targets discovered using this discovery address, enter the following:

```
Storage> iscsi discovery del discovery-address
```

where:

*discovery-address* The target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720.

You can specify either an IPv4 address or an IPv6 address. Optionally, you can specify a port with the IP address. For example:

```
192.168.0.4  
192.168.0.4:3260  
2001:c90::211:9ff:feb8:a9e9  
[2001:c90::211:9ff:feb8:a9e9]:3260
```

If no port is specified, the default port 3260 is used. Verify that your firewall allows you to access the target location through the port. For example:

```
# telnet discovery-address 3260
```

For example:

```
Storage> iscsi discovery del 192.168.2.15:3260
```

- 2 To verify the deletion of the discovery address, display the discovery addresses.

```
Storage> iscsi discovery list
```

```
Discovery Address  
-----  
192.168.2.14:3260
```

### To rediscover an iSCSI discovery address

- ◆ To rediscover an iSCSI discovery address, enter the following:

```
Storage> iscsi discovery rediscover discovery-address
```

where:

*discovery-address* The target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720.

You can specify either an IPv4 address or an IPv6 address.

Optionally, you can specify a port with the IP address. For example:

```
192.168.0.4  
192.168.0.4:3260  
2001:c90::211:9ff:feb8:a9e9  
[2001:c90::211:9ff:feb8:a9e9]:3260
```

If no port is specified, the default port 3260 is used. Verify that your firewall allows you to access the target location through the port. For example:

```
# telnet discovery-address 3260
```

For example:

```
Storage> iscsi discovery rediscover 192.168.2.15:3260
```

```
Deleted targets
```

```
-----
```

```
iqn.2001-04.com.example:storage.disk5.sys3.xyz
```

```
New targets
```

```
-----
```

```
iqn.2001-04.com.example:storage.disk6.sys3.new.xyz
```

```
Logging into target iqn.2001-04.com.example:storage.disk6.sys3.new.xyz
```

**To rediscover changes in targets or LUNs at a discovery address**

- ◆ To rediscover changes in targets or LUNs at a discovery address, enter the following:

```
Storage> iscsi discovery rediscover_new discovery-address
```

where:

*discovery-address* The target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720.

You can specify either an IPv4 address or an IPv6 address.

Optionally, you can specify a port with the IP address. For example:

```
192.168.0.4  
192.168.0.4:3260  
2001:c90::211:9ff:feb8:a9e9  
[2001:c90::211:9ff:feb8:a9e9]:3260
```

If no port is specified, the default port 3260 is used. Verify that your firewall allows you to access the target location through the port. For example:

```
# telnet discovery-address 3260
```

New LUNs or targets discovered at *discovery-address* will be automatically added and logged into. This command does not discover any targets that have been deleted at *discovery-address*.

For example:

```
Storage> iscsi discovery rediscover_new 192.168.2.15:3260  
14% [||] Checking for new targets  
  
New targets  
-----  
iqn.2001-04.com.example:storage.disk7.sys3.new.xyz  
  
100% [#] Updating disk list
```

# Configuring the iSCSI targets

## To display the iSCSI targets

- ◆ To display the iSCSI targets, enter the following:

```
Storage> iscsi target list
```

For example:

```
Storage> iscsi target list
```

```
Target
```

```
-----
```

```
iqn.2001-04.com.example:storage.disk2.sys3.xyz  
iqn.2001-04.com.example:storage.disk4.sys3.xyz  
iqn.2001-04.com.example:storage.disk5.sys3.xyz  
iqn.2001-04.com.example:storage.disk3.sys3.xyz  
iqn.2001-04.com.example2:storage.disk2.sys3.xyz  
iqn.2001-04.com.example2:storage.disk3.sys3.xyz  
iqn.2001-04.com.example2:storage.disk4.sys3.xyz  
iqn.2001-04.com.example2:storage.disk5.sys3.xyz
```

```
Discovery Address  State  Disk  
-----  -
```

192.168.2.14:3260	ONLINE	disk_0
192.168.2.14:3260	ONLINE	disk_2
192.168.2.14:3260	ONLINE	disk_3
192.168.2.14:3260	ONLINE	disk_1
192.168.2.15:3260	ONLINE	disk_4
192.168.2.15:3260	ONLINE	disk_5
192.168.2.15:3260	ONLINE	disk_6
192.168.2.15:3260	ONLINE	disk_7

**To display the iSCSI target details**

- ◆ To display the iSCSI target details, enter the following:

```
Storage> iscsi target listdetail target
```

where *target* is the name of the node you want to display the details for.

This list also shows targets discovered at *discovery-address*, not only manually added targets.

For example:

```
Storage> iscsi target listdetail iqn.2001-04.com.example:
storage.disk2.sys3.xyz
```

```
Discovery Address : 192.168.2.14:3260
```

```
Connections
```

```
=====
```

Portal Address	ACCESS_01	ACCESS_02
-----	-----	-----
192.168.2.14:3260,1	2	2

### To add an iSCSI target

- ◆ To add an iSCSI target, enter the following:

```
Storage> iscsi target add target-name portal-address
```

**target-name** Name of the iSCSI target at which SCSI LUNs are available. *target-name* should conform to the naming rules defined in RFC3721.

**portal-address** The location where the target is accessible.  
 You can specify either an IPv4 address or an IPv6 address.

For example:

```
192.168.0.4
192.168.0.4,1
192.168.0.4:3260
192.168.0.4:3260,1
2001:c90::211:9ff:feb8:a9e9
2001:c90::211:9ff:feb8:a9e9,1
[2001:c90::211:9ff:feb8:a9e9]:3260
[2001:c90::211:9ff:feb8:a9e9]:3260,10
```

For example:

```
Storage> iscsi target add iqn.2001-04.com.example:  

storage.disk2.sys1.xyz 192.168.2.14:3260
```

Logging into target *iqn.2001-04.com.example*:

```
storage.disk2.sys1.xyz
```

```
Storage> iscsi target listdetail iqn.2001-04.com.example:  

storage.disk2.sys1.xyz
```

Connections

=====

Portal Address	ACCESS55_01	ACCESS55_02
-----	-----	-----
192.168.2.14:3260,1	1	1

### To delete an iSCSI target

- ◆ To delete an iSCSI target, enter the following:

```
Storage> iscsi target del target-name  
{discovery-address|portal-address}
```

**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** Target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720. If no port is specified with the discovery address, default port 3260 is used.

**portal-address** The location where the target is accessible.

For example:

```
Storage> iscsi target del iqn.2001-04.com.example:  
storage.disk2.sys3.xyz
```

### To login to an iSCSI target

- ◆ To login to an iSCSI target, enter the following:

```
Storage> iscsi target login target-name  
{discovery-address | portal-address}
```

**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** Target address at which an initiator can request a list of targets using a `SendTargets` text request as specified in iSCSI protocol of RFC3720. If no port is specified with the discovery address, default port 3260 is used.

**portal-address** The location where the target is accessible.

For example:

```
Storage> iscsi target login iqn.2001-04.com.example:  
storage.disk2.sys3.xyz
```

### To logout from an iSCSI target

- ◆ To logout from an iSCSI target, enter the following:

```
Storage> iscsi target logout target-name  
{discovery-address | portal-address}
```

**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**    Target address at which an initiator can request a list of targets  
                          using a `SendTargets` text request as specified in iSCSI protocol  
                          of RFC3720. If no port is specified with the discovery address,  
                          default port 3260 is used.

**portal-address**        The location where the target is accessible.

For example:

```
Storage> iscsi target logout iqn.2001-04.com.example:  
storage.disk2.sys3.xyz
```

### To rescan targets for new LUNs

- ◆ To rescan a target for a new LUN, enter the following:

```
Storage> iscsi target rescan target-name
```

where *target-name* is the name of the iSCSI target that you want to rescan.

You can use the `Storage> iscsi target rescan` command for both static targets and discovered targets.

For example:

```
Storage> iscsi target rescan iqn.2001-04.com.example:storage.disk2  
.sys3.xyz
```

```
100% [#] Updating disk list
```

```
Storage> iscsi target list
```

```
Target
```

```
-----
```

```
iqn.2001-04.com.example:storage.disk2.sys3.xyz  
iqn.2001-04.com.example:storage.disk4.sys3.xyz  
iqn.2001-04.com.example:storage.disk5.sys3.xyz  
iqn.2001-04.com.example:storage.disk3.sys3.xyz  
iqn.2001-04.com.example2:storage.disk2.sys3.xyz  
iqn.2001-04.com.example2:storage.disk3.sys3.xyz  
iqn.2001-04.com.example2:storage.disk4.sys3.xyz  
iqn.2001-04.com.example2:storage.disk5.sys3.xyz
```

Discovery Address	State	Disk
-----	-----	----
192.168.2.14:3260	ONLINE	disk_0 disk_8 disk_9
192.168.2.14:3260	ONLINE	disk_2
192.168.2.14:3260	ONLINE	disk_3
192.168.2.14:3260	ONLINE	disk_1
192.168.2.15:3260	ONLINE	disk_4
192.168.2.15:3260	ONLINE	disk_5
192.168.2.15:3260	ONLINE	disk_6
192.168.2.15:3260	ONLINE	disk_7

## Modifying tunables for iSCSI

You can set the values of the attributes on the targets. You can set or show the default values, the values for all targets, or the values for a specific target.

[Table 8-1](#) shows the target attributes that you can modify.

**Table 8-1** Attributes for iSCSI targets

Attribute	Description
cmds_max	The maximum number of SCSI commands that the session will queue. A session is defined as a connection between the initiator and 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.
fast_abort	Defines whether 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 or No.
initial_login_retry_max	The maximum number of times that the iSCSI initiator should try a login to the target during 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.
login_timeout	The amount of time that the iSCSI initiator service should wait for login to complete. The value of this attribute is in seconds. Valid values range from 10 to 600.
logout_timeout	The amount of time that 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.
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.
noop_timeout	The amount of time that the iSCSI initiator service should wait for response to a Nop-out request sent to the target, before failing the connection. Failing the connection causes the 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.
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.

**Table 8-1** Attributes for iSCSI targets (*continued*)

Attribute	Description
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.

**To display the default value for target attributes**

- ◆ To display the default value for target attributes, enter the following:

```
Storage> iscsi target attr showdefault
```

For example:

```
Storage> iscsi target attr showdefault
Attribute          Value
-----
replacement_timeout 122
noop_timeout       5
noop_interval      13
login_timeout      10
logout_timeout     15
cmds_max           128
queue_depth        32
initial_login_retry_max 10
fast_abort         No
```

**To display values for target attributes of all known targets**

- ◆ To display values for target attributes of all known targets, enter the following:

```
Storage> iscsi target attr showall
```

For example:

```
Storage> iscsi target attr showall
```

Attribute	Value	Target
-----	-----	-----
replacement_timeout	123	iqn.1992-08.com.iscsi:sn.84268871
noop_timeout	5	iqn.1992-08.com.iscsi:sn.84268871
noop_interval	121	iqn.1992-08.com.iscsi:sn.84268871
login_timeout	10	iqn.1992-08.com.iscsi:sn.84268871
logout_timeout	15	iqn.1992-08.com.iscsi:sn.84268871
cmds_max	128	iqn.1992-08.com.iscsi:sn.84268871
queue_depth	32	iqn.1992-08.com.iscsi:sn.84268871
initial_login_retry_max	5	iqn.1992-08.com.iscsi:sn.84268871
fast_abort	No	iqn.1992-08.com.iscsi:sn.84268871
replacement_timeout	124	iqn.2009-01.com.example:storage.disk0.lun0
noop_timeout	5	iqn.2009-01.com.example:storage.disk0.lun0
noop_interval	121	iqn.2009-01.com.example:storage.disk0.lun0
login_timeout	10	iqn.2009-01.com.example:storage.disk0.lun0
logout_timeout	15	iqn.2009-01.com.example:storage.disk0.lun0
cmds_max	128	iqn.2009-01.com.example:storage.disk0.lun0
queue_depth	32	iqn.2009-01.com.example:storage.disk0.lun0
initial_login_retry_max	10	iqn.2009-01.com.example:storage.disk0.lun0
fast_abort	No	iqn.2009-01.com.example:storage.disk0.lun0

**To display the attribute values for a specific target**

- ◆ To display the attribute values for a specific target, enter the following:

```
Storage> iscsi target attr show target-name
```

where *target-name* is the name of the iSCSI target to be displayed.

For example:

```
Storage> iscsi target attr show iqn.1992-08.com.iscsi:sn.84268871
Attribute                               Value
-----                               -
replacement_timeout                    123
noop_timeout                            5
noop_interval                           121
login_timeout                           10
logout_timeout                          15
cmds_max                                 128
queue_depth                             32
initial_login_retry_max                 5
fast_abort                               No
```

**To set the default value for a target attribute**

- ◆ To set the default value for a target attribute, enter the following:

```
Storage> iscsi target attr setdefault attribute value
```

*attribute*            The attribute for which to set the value.

*value*                The default value to be set for the attribute.

The default value is inherited by any new targets that get added.

For example:

```
Storage> iscsi target attr setdefault login_timeout 10
Success.
```

### To set an attribute value for all known targets

- ◆ To set an attribute value for all known targets, enter the following:

```
Storage> iscsi target attr setall attribute value
```

*attribute*            The attribute for which to set the value.

*value*                The value to be set for the attribute.

This command does not change the default value as shown in the `Storage> iscsi target attr showdefault` command. Changes to values are effective after re-login.

For example:

```
Storage> iscsi target attr setall logout_timeout 20
```

Changes would be applicable after next login into the target.  
Success.

### To set the attribute value for a specific target

- ◆ To set the attribute value for a specific target, enter the following:

```
Storage> iscsi target attr set target-name attribute value
```

*target-name*        The name of the specific iSCSI target.

*attribute*           The attribute of the specific target.

*value*                The value to be set for the target attribute.

For example:

```
Storage> iscsi target attr set iqn.1992-08.com.iscsi:sn.84268871 noop_interval 30
```

Changes would be applicable after next login into the target.  
Success.

# Configuring the cloud gateway

This chapter includes the following topics:

- [About the cloud gateway](#)
- [Configuring the cloud gateway](#)

## About the cloud gateway

You can configure Veritas Access as a gateway to cloud storage. You can register Amazon AWS S3 subscriptions to your Veritas Access cluster. Multiple cloud subscriptions can be attached, so you need to assign a service name to each subscription. You can then use the service name to attach the S3 subscription to a scale-out file system as a storage tier.

The cloud as a tier feature lets you have hybrid storage that uses both on-premises storage and public cloud storage. After the gateway and tier are configured, you can use the cloud as a tier feature to move data between the cloud and the on-premises storage. The files in the Amazon S3 cloud, like the files on the on-premises storage, are accessible using the NFS protocol. Access of the data present in the cloud tier is transparent to the application.

See [“Configuring the cloud as a tier feature for scale-out file systems”](#) on page 497.

Before you provision cloud storage, you set up Amazon AWS S3 subscriptions. To set up the cloud gateway, you attach Amazon AWS S3 subscriptions to your Veritas Access cluster. You need to have the subscription credentials to add the AWS S3 subscriptions. You need the Amazon AWS S3 access and secret keys.

# Configuring the cloud gateway

A cloud gateway enables you to register one or more cloud services to the cluster. You can add the cloud service as a cloud tier for a scale-out file system. Whenever you are adding a tier to a scale-out file system, you need to add a cloud service for the cloud tier. You require a cloud service for a scale-out file system.

## To configure the cloud service for scale-out file systems

- 1 Add the cloud service.

```
Storage> cloud addservice service_name service_provider=AWS
```

You are prompted to provide Amazon S3 subscription credentials.

- 2 Display the added cloud services.

```
Storage> cloud listservice service_name
```

- 3 Remove the cloud service.

```
Storage> cloud removeservice service_name
```

If any scale-out file system has a cloud tier associated with the service, the remove cloud service operation fails. Remove all the tiers from all the scale-out file systems before removing the cloud service.

# Managing Veritas Access file sharing services

- [Chapter 10. Configuring your NFS server](#)
- [Chapter 11. Using Veritas Access as a CIFS server](#)
- [Chapter 12. Using Veritas Access with Amazon S3](#)
- [Chapter 13. Configuring your FTP server](#)
- [Chapter 14. Configuring Veritas Access with OpenStack Cinder](#)
- [Chapter 15. Configuring Veritas Access with OpenStack Manila](#)
- [Chapter 16. Configuring Veritas Access to work with Oracle Direct NFS](#)

# Configuring your NFS server

This chapter includes the following topics:

- [About using NFS server with Veritas Access](#)
- [Accessing the NFS server](#)
- [Displaying and resetting NFS statistics](#)
- [Configuring Veritas Access for ID mapping for NFS version 4](#)
- [Configuring the NFS client for ID mapping for NFS version 4](#)
- [About authenticating NFS clients](#)
- [Setting up Kerberos authentication for NFS clients](#)

## About using NFS server with Veritas Access

Veritas Access provides file access services to UNIX and Linux client computers using the Network File System (NFS) protocol. Veritas Access file systems can be exported over NFS v3 or NFS v4. Veritas Access provides the following NFS server support:

- NFS-Ganesha server  
See [“Using the NFS-Ganesha server”](#) on page 142.
- Kernel-based NFS server  
See [“Using the kernel-based NFS server”](#) on page 142.

At any time, either NFS-Ganesha or kernel NFS is active. The kernel NFS server is enabled by default. If required, you can switch the NFS server that you use.

See [“Switching between NFS servers”](#) on page 143.

## Using the kernel-based NFS server

The kernel-based NFS server supports NFS version 3. The kernel NFS server is enabled by default. Kernel NFS supports Active-Active mode serving NFS version 3. Veritas recommends that you use the default kernel-based NFS server unless you require NFS version 4 support.

## Using the NFS-Ganesha server

If you plan to use NFS version 4, you must use Veritas Access with an NFS-Ganesha server.

NFS-Ganesha provides support for both NFS version 3 and NFS version 4. NFS-Ganesha is a user-space implementation of the NFS server. The use of a NFS-Ganesha server is optional. NFS-Ganesha is not enabled by default.

For scale-out file systems with `largefs` layout, an NFS-Ganesha share is always exported from only one node in the cluster. This node can be any one of the nodes in the cluster. At the time of share export, the virtual IP address that is used for accessing the share is displayed. Different shares can be exported from different nodes. The shares are highly available in case of a node failure.

Certain limitations apply for NFS-Ganesha.

See [“NFS-Ganesha limitations”](#) on page 142.

Since the kernel-based NFS server is the default, switch the NFS server to NFS-Ganesha.

### NFS-Ganesha limitations

The following limitations apply for NFS-Ganesha:

- Clients cannot be added dynamically. Once an export is added, you cannot add more clients to the export. The workaround is to add a `netgroup` when you create the share. The `netgroup` membership can be changed dynamically. See [“About managing NFS shares using netgroups”](#) on page 414.
- The `fcntl` lock failover is not supported for NFS-Ganesha v3.
- Export options like `secure_locks`, `insecure_locks`, `wdelay`, `no_wdelay`, `subtree_check`, `no_subtree_check`, and `fsid` are not supported with NFS-Ganesha.
- NFS-Ganesha supports only OpenStack Cinder. It does not support OpenStack Manila.

- NFS v4 ACLs are not supported by Veritas Access.

## Switching between NFS servers

If NFS v4 is your primary use case, we recommend that you use the NFS-Ganesha server. You should also use the NFS-Ganesha server if you require Kerberos authentication. The NFS-Ganesha server supports both NFS v3 and NFS v4, and Kerberos authentication is supported for both NFS v3 and v4.

If NFS v3 is your primary use case, then we recommend that you use the kernel NFS server.

A CLISH command is provided to switch from kernel NFS server to NFS-Ganesha, or vice versa. Before you switch between the NFS servers, the NFS server must be offline.

All of the available NFS shares are moved from the previous NFS server to the new NFS server; therefore, the operation may be time consuming.

### To switch between NFS servers

- 1 Make sure that the NFS server is offline. You can view the status of the NFS server with the following command:

```
NFS> server status
```

- 2 Use the following command to switch the NFS server:

```
NFS> server switch
```

## Recommended tuning for NFS-Ganesha version 3 and version 4

Veritas Access supports both the NFS kernel-based server and the NFS-Ganesha server in a mutually exclusive way. The NFS kernel-based server supports NFS version 3 only. The NFS-Ganesha server supports both NFS version 3 and NFS version 4.

See [“Using the NFS-Ganesha server”](#) on page 142.

The NFS-Ganesha server does not run in the kernel, instead NFS-Ganesha runs in user space on the NFS server. This means that the NFS-Ganesha server processes can be affected by system resource limitations as any other user space process can be affected. There are some NFS-server operating system tuning values that you should modify to ensure that the NFS-Ganesha server performance is not unduly affected. You use the NFS client mount option `version` to determine whether NFS version 3 or NFS version 4 is used. On the NFS client, you can select either the `version=3` or the `version=4` mount option. The NFS client is unaware

of whether the NFS server is using kernel-based NFS or NFS-Ganesha. Only if NFS-Ganesha is enabled in Veritas Access can a client perform an NFS mount using the mount option of `version=4`.

When you start a system, `kswapd_init()` calls a kernel thread that is called `kswapd`, which continuously executes the function `kswapd()` in `mm/vmscan.c` that usually sleeps. The `kswapd` daemon is responsible for reclaiming pages when memory is running low. `kswapd` performs most of the tasks that are needed to maintain the page cache correctly, shrink slab caches, and swap out processes if necessary. `kswapd` keeps freeing pages until the `pages_high` watermark is reached. Under extreme memory pressure, processes do the work of `kswapd` synchronously by calling `balance_classzone()`, which calls the `try_to_free_pages_zone()`.

When there is memory pressure, pages are claimed using two different methods.

- `pgscank/s` – The `kswapd` kernel daemon periodically wakes up and claims (frees) memory in the background when free memory is low. `pgscank/s` records this activity.
- `pgscand/s` – When `kswapd` fails to free up enough memory, then the memory is also claimed directly in the process context (thus blocking the user program execution). `pgscand/s` records this activity.
- The total pages being claimed (also known as page stealing) is therefore a combination of both `pgscank/s` and `pgscand/s`. `pgsteal/s` records the total activity, so  $(pgsteal/s = pgscank/s + pgscand/s)$ .

The NFS-Ganesha user process can be affected when `kswapd` fails to free up enough memory. To alleviate the possibility of the NFS-Ganesha process from doing the work of `kswapd`, Veritas recommends increasing the value of the Linux virtual machine tunable `min_free_kbytes`.

Example of a default auto-tuned value:

```
sysctl -a | grep vm.min_free
vm.min_free_kbytes = 90112
```

You use `min_free_kbytes` to force the Linux VM (virtual memory management) to keep a minimum number of kilobytes free. The VM uses this number to compute a watermark value for each `lowmem` zone in the system.

**Table 10-1** Recommended tuning parameters for NFS version 3 and version 4

Option	Description
NFS mount options	<p>File system mount options for the NFS client:</p> <ul style="list-style-type: none"> <li>■ <code>version=3/4</code></li> <li>■ <code>nordirplus</code></li> <li>■ <code>sharecache</code></li> </ul>
NFS server export options	<p>NFS server export options:</p> <ul style="list-style-type: none"> <li>■ <code>rw</code></li> <li>■ <code>sync</code></li> <li>■ <code>no_root_squash</code></li> </ul>
Jumbo frames	<p>A jumbo frame is an Ethernet frame with a payload greater than the standard maximum transmission unit (MTU) of 1,500 bytes. Enabling jumbo frames improves network performance in I/O intensive workloads. If jumbo frames are supported by your network, and if you wish to use jumbo frames, Veritas recommends using a jumbo frame size of 5000.</p>
<code>min_free_kbytes</code>	<p>On server nodes with 96 GB RAM or more, the recommended value of <code>min_free_kbytes</code> is 1048576 (=1 GB). On server nodes using the minimum of 32 GB RAM, the minimum recommended value of <code>min_free_kbytes</code> is 524288 (=512 MB).</p>

# Accessing the NFS server

## To check on the NFS server status

- ◆ Prior to starting the NFS server, check on the status of the server by entering:

```
NFS> server status
```

The output shows the status. The output also indicates whether the NFS server used is the kernel NFS server or the NFS-Ganesha server.

For example, for the kernel NFS server:

```
NFS> server status
NFS Status on access_01 : OFFLINE
NFS Status on access_02 : OFFLINE
```

For example, for the NFS-Ganesha server:

```
NFS> server status
GNFS Status on access_01 : OFFLINE
GNFS Status on access_02 : OFFLINE
```

The states (ONLINE, OFFLINE, and FAULTED) correspond to each Veritas Access node identified by the node name. The states of the node may vary depending on the situation for that particular node.

The possible states of the `NFS> server status` command are:

ONLINE	Indicates that the node can serve NFS protocols to the client.
OFFLINE	Indicates the NFS services on that node are down.
FAULTED	Indicates something is wrong with the NFS service on the node.

You can run the `NFS> server start` command to restart the NFS services, and only the nodes where NFS services have problems, are restarted.

### To start the NFS server

- ◆ To start the NFS server, enter the following:

```
NFS> server start
```

You can use the `NFS> server start` command to clear an OFFLINE state from the `NFS> server status` output by only restarting the services that are offline. You can run the `NFS> server start` command multiple times without it affecting the already-started NFS server.

For example:

```
NFS> server start
..Success.
```

Run the `NFS> server status` command again to confirm the change.

```
NFS> server status
NFS Status on access_01 : ONLINE
NFS Status on access_02 : ONLINE
```

### To stop the NFS server

- ◆ To stop the NFS server, enter the following:

```
NFS> server stop
```

For example:

```
NFS> server stop
..Success.
```

## Displaying and resetting NFS statistics

The NFS statistics shown differ depending on whether the NFS server is the default kernel NFS server, or the NFS-Ganesha server.

Veritas Access does not support resetting the NFS statistics for the NFS-Ganesha server.

### To display statistics for a specific node or for all the nodes in the cluster

To display NFS statistics, enter the following:

```
NFS> stat show [nodename]
```

where *nodename* specifies the node name for which you are trying to obtain the statistical information. If the *nodename* is not specified, statistics for all the nodes in the cluster are displayed.

For example, to display the NFS statistics for all the nodes in the cluster for the kernel NFS server, enter the following:

```
NFS> stat show all
node_01
-----
Server rpc stats:
calls      badcalls   badauth    badclnt    xdrcll
3142       0          0          0          0

Server nfs:
null       getattr    setattr    lookup     access     readlink
6          0% 4      0% 0      0% 0      0% 4      0% 0      0%
read      write      create     mkdir      symlink    mknod
0          0% 3125   99% 0      0% 0      0% 0      0% 0      0%
remove    rmdir     rename     link       readdir    readdirplus
0          0% 0      0% 0      0% 0      0% 0      0% 1      0%
fsstat    fsinfo    pathconf   commit
0          0% 1      0% 0      0% 1      0%

node_02
-----
Server rpc stats:
calls      badcalls   badauth    badclnt    xdrcll
322       0          0          0          0

Server nfs:
null       getattr    setattr    lookup     access     readlink
1          0% 2      0% 1      0% 1      0% 2      0% 0      0%
read      write      create     mkdir      symlink    mknod
0          0% 313   97% 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%
fsstat    fsinfo    pathconf   commit
0          0% 1      0% 0      0% 1      0%

node.NFS>
```

For example, to display the NFS statistics for all the nodes in the cluster for the NFS-Ganesha server, enter the following:

```
NFS> stat show all
node_01
```

```
-----  
EXPORT PATH PROTO TYPE REQ (MB) XFER (MB) TOTAL OPS AVG LATENCY (ms)  
/vx/fs1 NFSv3 READ 0.00 0.00 0 0.00  
/vx/fs1 NFSv3 WRITE 48.00 48.00 48 11.85  
/vx/fs1 NFSv4 READ 0.00 0.00 0 0.00  
/vx/fs1 NFSv4 WRITE 100.00 100.00 100 8.42  
node_02  
-----  
EXPORT PATH PROTO TYPE REQ (MB) XFER (MB) TOTAL OPS AVG LATENCY (ms)  
/vx/fs1 NFSv3 READ 1.00 0.00 0 0.00  
/vx/fs1 NFSv3 WRITE 51.00 78.00 53 17.85  
/vx/fs1 NFSv4 READ 9.00 0.00 0 0.00  
/vx/fs1 NFSv4 WRITE 108.00 116.00 111 9.42  
node.NFS>
```

### To reset NFS statistics for a specific node or for all the nodes in the cluster to zero

- ◆ To reset NFS statistics for the kernel NFS server, enter the following:

```
NFS> stat reset [nodename]
```

where *nodename* specifies the node name for which you want to reset the NFS statistics to zero. If *nodename* is not specified, NFS statistics for all the nodes in the cluster are reset to zero. Statistics are automatically reset to zero after a reboot of a node, or in the case of NFS-Ganesha, after you reboot the node or the NFS server restarts.

For example, to reset NFS statistics on *node\_02*, enter the following:

```
NFS> stat reset node_02  
Success.
```

## Configuring Veritas Access for ID mapping for NFS version 4

If you plan to use NFS version 4, you must configure Veritas Access to map the user IDs to the required format. In NFS version 3, each user is identified by a number, the user ID (uid). A UNIX file also identifies the owner of the file by a number. NFS version 4 has a different way of identifying users than that used by NFS version 3. In NFS version 4, each user is identified by a string, such as `user1@example.com`.

Veritas Access requires a mechanism to map the user strings from NFS version 4 to uids on the server and the client. This process, called ID mapping, uses a file `/etc/idmapd.conf`.

NFS-Ganesha uses the `/etc/idmapd.conf` file to map the IDs. The Domain field needs to be set to the DNS domain of the Veritas Access server. If the DNS domain is not set, the ID mapping maps all of the users on the client to the user 'nobody'.

### To configure Veritas Access for ID mapping

- ◆ Configure the DNS domain of Veritas Access using the following command:

```
Network> dns set domainname domainname
```

For example:

```
Network> dns set domainname example.com
ACCESS dns INFO V-288-0 dns set domainname successful.
```

When the NFS version 4 server is started, the `/etc/idmapd.conf` file is updated with the domain information of the Veritas Access server.

You must also configure the NFS client.

See [“Configuring the NFS client for ID mapping for NFS version 4”](#) on page 150.

## Configuring the NFS client for ID mapping for NFS version 4

For NFS version 4, you must configure the NFS client so that the NFS version 4 user strings can be mapped to the uids. You must also configure the NFS server.

See [“Configuring Veritas Access for ID mapping for NFS version 4”](#) on page 149.

### To configure the NFS client for ID mapping

- 1 For proper ID mapping, set the `Domain` field in the `/etc/idmapd.conf` file as the DNS domain name of the NFS client. Make sure that the DNS domain is the same for the NFS client and the Veritas Access server.

This setting in the `/etc/idmapd.conf` file should be updated on the NFS client.

Example:

```
Domain = EXAMPLE.COM
```

- 2 Clear the ID mapping cache on the NFS client using the command `nfsidmap -c` and restart the ID mapping service.

```
Service rpcidmapd start
```

## About authenticating NFS clients

You can set up netgroups to provide authentication for NFS clients.

See “[About managing NFS shares using netgroups](#)” on page 414.

For the NFS-Ganesha server, you can also use Kerberos authentication.

Kerberos authentication is not supported with the kernel NFS server.

## Setting up Kerberos authentication for NFS clients

Kerberos provides a secure way of authenticating NFS clients. Veritas Access supports Kerberos authentication for NFS mounts if Veritas Access is running NFS-Ganesha. NFS-Ganesha is an NFS file server that runs in user mode on most UNIX or Linux systems. In this configuration, the Veritas Access server behaves as a Kerberos client. The Kerberos KDC (Key Distribution Center) server must already be set up and running outside of Veritas Access. For NFS version 3, when a Veritas Access share is exported with the `krb5` security option, the NFS clients have to mount the Veritas Access share with the `krb5` mount option. Otherwise the mount fails with an authentication error. For NFS version 4, the NFS clients automatically find the security type and mount the Veritas Access share with the same mount option.

---

**Note:** When CIFS security is configured with `ads`, Kerberos for NFS cannot be configured. When NFS is configured for Kerberos authentication, CIFS security cannot be configured with `ads`.

---

To configure Veritas Access for authenticating NFS clients using Kerberos, perform the tasks in the order that is listed in [Table 10-2](#).

**Table 10-2** Tasks for configuring Veritas Access for authenticating NFS clients using Kerberos

Task	Where to find more information
Add and configure Veritas Access to the Kerberos realm	See <a href="#">“Adding and configuring Veritas Access to the Kerberos realm”</a> on page 152.
Configure the NFS server for ID mapping	See <a href="#">“Configuring Veritas Access for ID mapping for NFS version 4”</a> on page 149.
Configure the NFS client for ID mapping	See <a href="#">“Configuring the NFS client for ID mapping for NFS version 4”</a> on page 150.
Exporting an NFS share for Kerberos authentication	See <a href="#">“Exporting an NFS share for Kerberos authentication”</a> on page 410.
Mount the NFS share from the NFS client	See <a href="#">“Mounting an NFS share from the NFS client”</a> on page 411.

## Adding and configuring Veritas Access to the Kerberos realm

Kerberos authentication support on Veritas Access is available only if the Key Distribution Center (KDC) server is running on a standalone computer (in a non-AD (Active Directory) environment), and there is a single KDC server. Before Veritas Access can be used as a Kerberos client, the NFS service principal of Veritas Access has to be added to the KDC server. Use the Veritas Access cluster name (either the short name or the fully qualified domain name) in small letters as the host name when creating the NFS service principal.

For example, if `access_ga_01` and `access_ga_02` are two nodes in the Veritas Access cluster, then `access_ga` (or the fully qualified domain name `access_ga.example.com`) should be used for adding the NFS service principal. The Domain Name System (DNS) or `/etc/hosts` is then set up to resolve `access_ga` to all the virtual IPs of the Veritas Access cluster.

### To configure the KDC server

- 1 Create the NFS service principal on the KDC server using the `kadmin.local` command.

```
addprinc -randkey nfs/access_ga
```

- 2 Create a `keytab` file for the NFS service principal on KDC.

```
ktadd -k /etc/access.keytab nfs/access_ga
```

- 3 Copy the created `keytab` file (`/etc/access.keytab`) to the Veritas Access console node.

- 4 Use the `Network> krb standalone set` command to set the Kerberos configuration on Veritas Access.

The `Network> krb standalone set` command takes the KDC server name, Kerberos realm, and the location of the `keytab` that is located on the Veritas Access console node. This command sets up the Kerberos configuration file `/etc/krb5.conf` with the KDC server name and realm on all the nodes of the Veritas Access cluster. The command then copies the `keytab` file to `/etc/krb5.keytab` on all the nodes of the Veritas Access cluster.

```
Network> krb standalone set kdc_server TESTKDC.COM /home/support/krb5.keytab
```

The `Network> krb standalone set` command checks for the correct domain in the `/etc/idmapd.conf` file. If the domain is not set, the command gives a warning message saying that the DNS domain name needs to be set.

See [“Configuring Veritas Access for ID mapping for NFS version 4”](#) on page 149.

**5** Use the `Network> krb standalone show` command to show the Kerberos configuration.

```
Network> krb standalone show
Kerberos General Info:
=====
KDC:      kdc_server
REALM:    TESTKDC.COM

Keytab Info:
=====
Keytab name: FILE:/etc/krb5.keytab
KVNO Timestamp          Principal
-----
2 07/07/15 16:02:54 nfs/access_fa@TESTKDC.COM (aes256-cts-hmac-shal-96)
2 07/07/15 16:02:54 nfs/access_fa@TESTKDC.COM (aes128-cts-hmac-shal-96)
2 07/07/15 16:02:54 nfs/access_fa@TESTKDC.COM (des3-cbc-shal)
2 07/07/15 16:02:54 nfs/access_fa@TESTKDC.COM (arcfour-hmac)
2 07/07/15 16:02:54 nfs/access_fa@TESTKDC.COM (des-hmac-shal)
2 07/07/15 16:02:55 nfs/access_fa@TESTKDC.COM (des-cbc-md5)
```

**6** Use the following commands to stop and restart the NFS-Ganesha service:

```
NFS> server stop
NFS> server start
```

**7** Use the `Network> krb standalone unset` command to reset the Kerberos configuration.

```
Network> krb standalone unset
ACCESS krb SUCCESS V-288-999 Kerberos configuration is reset

Network> krb standalone show
Kerberos is not configured
```

After the KDC server is configured, you can export the NFS shares with Kerberos authentication options.

See [“Exporting an NFS share for Kerberos authentication”](#) on page 410.

# Using Veritas Access as a CIFS server

This chapter includes the following topics:

- [About configuring Veritas Access for CIFS](#)
- [About configuring CIFS for standalone mode](#)
- [Configuring CIFS server status for standalone mode](#)
- [Changing security settings](#)
- [Changing security settings after the CIFS server is stopped](#)
- [About Active Directory \(AD\)](#)
- [About configuring CIFS for Active Directory \(AD\) domain mode](#)
- [About setting NTLM](#)
- [Setting NTLM](#)
- [About setting trusted domains](#)
- [About storing account information](#)
- [Storing user and group accounts](#)
- [About reconfiguring the CIFS service](#)
- [Reconfiguring the CIFS service](#)
- [About mapping user names for CIFS/NFS sharing](#)
- [About the mapuser commands](#)

- [Adding, removing, or displaying the mapping between CIFS and NFS users](#)
- [Automatically mapping of UNIX users from LDAP to Windows users](#)
- [About managing home directories](#)
- [About CIFS clustering modes](#)
- [About migrating CIFS shares and home directories](#)
- [Setting the CIFS aio\\_fork option](#)
- [About managing local users and groups](#)
- [Enabling CIFS data migration](#)

## About configuring Veritas Access for CIFS

The Common Internet File System (CIFS), also known as the Server Message Block (SMB), is a network file sharing protocol that is widely used on Microsoft and other operating systems. Veritas Access supports the SMB3 protocol.

You can specify either an IPv4 address or an IPv6 address.

Veritas Access supports the following clustering modes:

- Normal
- Clustered Trivial Database (CTDB) - a cluster implementation of the TDB (Trivial database) based on the Berkeley database API

Veritas Access supports the following CIFS security modes:

- User
- ADS

Each clustering mode supports both of the CIFS security modes. The ctdb clustering mode is a different clustered implementation of Veritas Access CIFS, which supports almost all of the features supported by normal clustering mode as well as some additional features.

Additional features supported in ctdb clustering mode:

- Directory-level share support and also supported in normal clustering mode
- Multi-instance share export of a file system/directory
- Simultaneous access of a share from multiple nodes and therefore better load balancing

See [“About CIFS clustering modes”](#) on page 210.

Veritas Access can be integrated into a network that consists of machines running Microsoft Windows. You can control and manage the network resources by using Active Directory (AD) domain controllers.

Before you use Veritas Access with CIFS, you must have administrator-level knowledge of the Microsoft operating systems, Microsoft services, and Microsoft protocols (including AD and NT services and protocols).

You can find more information about them at: [www.microsoft.com](http://www.microsoft.com).

When serving the CIFS clients, Veritas Access can be configured to operate in one of the operating mode environments described in [Table 11-1](#).

**Table 11-1** CIFS operating mode environments

Mode	Definition
Standalone	Information about the user and group accounts is stored locally on Veritas Access. Veritas Access also authenticates users locally using the Linux password and group files. This mode of operation is provided for Veritas Access testing and may be appropriate in other cases, for example, when Veritas Access is used in a small network and is not a member of a Windows security domain. In this mode of operation, you must create the local users and groups; they can access the shared resources subject to authorization control.
Active Directory (AD)	Veritas Access becomes a member of an AD security domain and is configured to use the services of the AD domain controller, such as DNS, LDAP, and NTP. Kerberos, NTLMv2, or NTLM authenticate users.

When Veritas Access operates in the AD domain mode, it acts as a domain member server and not as the domain controller.

## About configuring CIFS for standalone mode

If you do not have an AD server, you can use Veritas Access as a standalone server. Veritas Access is used in standalone mode when testing Veritas Access functionality and when it is not a member of a domain.

Before you configure the CIFS service for the standalone mode, do the following:

- Make sure that the CIFS server is not running.
- Set security to user.
- Start the CIFS server.

To make sure that the configuration has changed, do the following:

- Check the server status.

- Display the server settings.

## Configuring CIFS server status for standalone mode

### To check the CIFS server status

- 1 To check the status of the CIFS server, enter the following:

```
CIFS> server status
```

By default, `security` is set to `user`, the required setting for standalone mode. The following example shows that `security` was previously set to `ads`.

For example:

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

Homedirfs           : fsl
Security             : ads
Domain membership status : Disabled
Domain               : VERITASDOMAIN.COM
Domain Controller    : VRTSSERVER
Domain User          : administrator
Clustering Mode      : normal
```

- 2 If the server is running, enter the following:

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

## To check the security setting

- 1 To check the current settings before setting security, enter the following:

```
CIFS> show
```

For example:

Name	Value
----	-----
netbios name	mycluster
ntlm auth	yes
allow trusted domains	no
homedirfs	
aio size	1024
idmap backend	rid:10000-1000000
workgroup	VERITASDOMAIN
security	ads
Domain	VERITASDOMAIN.COM
Domain user	administrator
Domain Controller	VRTSSERVER
Clustering Mode	normal

- 2 To set security to `user`, enter the following:

```
CIFS> set security user
```

Global option updated. Note: Restart the CIFS server.

**To start the CIFS service in standalone mode**

- 1 To start the service in standalone mode, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

- 2 To display the new settings, enter the following:

```
CIFS> show
```

For example:

Name	Value
----	-----
netbios name	mycluster
ntlm auth	yes
allow trusted domains	no
homedirfs	
aio size	1024
idmap backend	rid:10000-1000000
workgroup	VERITASDOMAIN
security	user
Domain	VERITASDOMAIN.COM
Domain user	administrator
Domain Controller	VRTSSERVER
Clustering Mode	normal

- 3 To make sure that the server is running in standalone mode, enter the following:

```
CIFS> server status
```

For example:

```
CIFS> server status  
CIFS Status on test_01 : ONLINE  
CIFS Status on test_02 : ONLINE  
  
Homedirfs : fs1  
Security : user  
Clustering Mode : normal
```

The CIFS service is now running in standalone mode.

See [“About managing local users and groups”](#) on page 224.

See [“About managing CIFS shares”](#) on page 421.

## Changing security settings

### To change security settings

- ◆ To set the security to user, enter the following:

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

### To stop the CIFS server:

```
CIFS> server stop
Disabling membership in existing domain VERITASDOMAIN.COM

Enter password for user 'administrator' of domain
VERITASDOMAIN.COM :
Stopping CIFS Server.....Success.
Left domain VERITASDOMAIN.COM
```

## Changing security settings after the CIFS server is stopped

### To change security settings for a CIFS server that has been stopped

- ◆ To set security to a value other than `domain`, enter the following:

```
CIFS> set security user
Disabling membership in existing domain VERITASDOMAIN.COM

Enter password for user 'administrator' of domain
VERITASDOMAIN.COM :
Left domain VERITASDOMAIN.COM
Global option updated. Note: Restart the CIFS server.
```

If the server is stopped, then changing the security mode will disable the membership of the existing domain.

## About Active Directory (AD)

In order to provide CIFS services, Veritas Access must be able to authenticate within the Windows environment.

Active Directory (AD) is a technology created by Microsoft that provides a variety of network services including LDAP directory services, Kerberos-based

authentication, Domain Name System (DNS) naming, secure access to resources, and more.

Veritas Access will not join the AD domain if its clock is excessively out-of-sync with the clock on the AD domain controller. Ensure that Network Time Protocol (NTP) is configured on Veritas Access, preferably on the same NTP server as the AD domain controller.

See [“Coordinating cluster nodes to work with NTP servers”](#) on page 85.

## Configuring entries for Veritas Access DNS for authenticating to Active Directory (AD)

Name resolution must be configured correctly on Veritas Access. Domain Name System (DNS) is usually used for name resolution.

### **To configure entries for Veritas Access DNS for authenticating to Active Directory**

- 1 Create an entry for the Veritas Access cluster name.

The cluster name is chosen at the time of installation, and it cannot be reset afterwards. It is also the NetBios name of the cluster, hence it must resolve to an IP address.

- 2 Configure the Veritas Access cluster name in DNS so that queries to it return the Virtual IP Addresses (VIPs) associated with the Veritas Access cluster in a round-robin fashion.

This is done by creating separate A records that map the cluster name to each VIP. So, if there are four VIPs associated with the Veritas Access cluster (not including special VIPs for backup, replication for Veritas Access, and so on), then there must be four A records mapping the cluster name to the four VIPs.

- 3 Verify that the DNS server has correct entries for Veritas Access by querying from a client:

```
myclient:~ # nslookup myaccess
Server:          10.182.108.75
Address:         10.182.108.75#53

Name:   myaccess.accesstest-ad2.local
Address: 10.182.96.31
Name:   myaccess.accesstest-ad2.local
Address: 10.182.96.30
Name:   myaccess.accesstest-ad2.local
Address: 10.182.96.29
Name:   myaccess.accesstest-ad2.local
Address: 10.182.96.28
```

In the above scenario, the DNS server at 10.182.108.75, with domain name `accesstest-ad2.local`, has been configured so that queries for `myaccess.accesstest-ad2.local` rotate in a round-robin manner among IP addresses ranging from 10.182.96.28 through 10.182.96.31. All of these are VIPs associated with the Veritas Access cluster named `myaccess`.

After configuring the DNS server correctly, Veritas Access must be configured as a DNS client.

This is done during installation, but may be modified by using the following commands:

```
Network> dns set domainname accesstest-ad2.local

Network> dns set nameservers 10.182.108.75

Network> dns enable
```

- 4 Verify that DNS client parameters are set correctly by entering the following command:

```
Network> dns show
```

- 5 Ensure host resolution is querying DNS by checking nsswitch:

```
Network> nsswitch show
hosts:  files      dns
```

In the above scenario, host resolution first looks at files, and then DNS.

Configuring name resolution correctly is critical in order to successfully join Veritas Access to Active Directory.

## Joining Veritas Access to Active Directory (AD)

### To join Veritas Access to Active Directory (AD)

- 1 To stop the CIFS server, enter the following command.

```
CIFS> server stop
```

- 2 To set the domain, enter the following command:

```
CIFS> set domain accesstest-ad2.local
```

In this example, it is the same as the DNS domain name.

This is the domain name of Active Directory.

- 3 To set the domain controller, enter the following command:

```
CIFS> set domaincontroller 10.182.108.75
```

In this example, it is the same as the DNS server that was configured earlier.

This is the IP address of the Active Directory Domain Controller. However, this is not a requirement . The DNS server and Active Directory can run on different servers, and hence this IP address may be different from the IP address of the DNS server.

- 4 To set the domain user, enter the following command:

```
CIFS> set domainuser newuser
```

This is a user whose credentials are used to join the Active Directory domain. The `domainuser` must have Domain Join privilege into the Active Directory domain. The `domainuser` need not be Administrator.

- 5 To set the CIFS security mode, enter the following command:

```
CIFS> set security ads
```

The other CIFS security mode is `user` for local users. For authenticating to Active Directory, use the `ads` CIFS security mode.

- 6 To start the CIFS server, enter the following command:

```
CIFS> server start
```

Veritas Access displays the time on the cluster as well as the time on the Active Directory Domain Controller.

If NTP has been configured correctly, then there will be no time skew.

Otherwise, you will need to reconfigure NTP correctly.

You will be prompted to enter the password of `domainuser`.

## Verifying that Veritas Access has joined Active Directory (AD) successfully

### To verify that Veritas Access has joined Active Directory (AD) successfully

- ◆ To verify that Veritas Access has joined Active Directory successfully, enter the following command:

```
CIFS> server status
```

For example:

```
CIFS> server status
CIFS Status on ctddb_01 : ONLINE
CIFS Status on ctddb_02 : ONLINE

Homedirfs           : fs2,fs6
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VRTSSERVER
Domain User         : administrator
Clustering Mode     : normal
```

Refer to the `Domain membership status` line of the output to verify that the Veritas Access cluster has joined the domain (displays as `Enabled`) if the join is successful.

If the cluster did not join the domain, an informative error message is provided indicating why the Veritas Access cluster cannot join the domain.

## About configuring CIFS for Active Directory (AD) domain mode

This section assumes that an Active Directory (AD) domain has already been configured and that Veritas Access can communicate with the AD domain controller (DC) over the network. The AD domain controller is also referred to as the AD server.

## Configuring CIFS for the AD domain mode

### To set the domain user for AD domain mode

- 1 To verify that the CIFS server is stopped, enter the following:

```
CIFS> server status
```

- 2 If the server is running, stop the server. Enter the following:

```
CIFS> server stop
```

- 3 To set the domain user, enter the following:

```
CIFS> set domainuser username
```

where *username* is the name of an existing AD domain user who has permission to perform the join domain operation.

For example:

```
CIFS> set domainuser administrator
```

Global option updated. Note: Restart the CIFS server.

### To set the domain for AD domain mode

- ◆ To set the domain for AD domain mode, enter the following:

```
CIFS> set domain domainname
```

where *domainname* is the name of the domain.

For example:

```
CIFS> set domain VERITASDOMAIN.COM
```

Global option updated. Note: Restart the CIFS server.

### To set the domain controller for AD domain mode

- ◆ To set the domain controller, enter the following:

```
CIFS> set domaincontroller servername
```

where *servername* is the server's IP address or DNS name.

For example, if the server SYMSERVER has an IP address of 172.16.113.118, you can specify one of the following:

```
CIFS> set domaincontroller 172.16.113.118
```

Global option updated. Note: Restart the CIFS server.

or

```
CIFS> set domaincontroller SYMSERVER
```

Global option updated. Note: Restart the CIFS server.

### To set security to ads

- ◆ To set security to ads, enter the following:

```
CIFS> set security ads|user
```

Enter *ads* for *security*.

```
CIFS> set security ads
```

Global option updated. Note: Restart the CIFS server.

### To set the workgroup

- ◆ To set the workgroup name if the WORKGROUP or NetBIOS domain name is different from the domain name, enter the following:

```
CIFS> set workgroup workgroup
```

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

For example, if SIMPLE is the name of the WORKGROUP you want to set, you would enter the following:

```
CIFS> set workgroup SIMPLE
```

Though the following symbols \$, (, ', and & are valid characters for naming a WORKGROUP, the Veritas Access CIFS implementation does not allow using these symbols.

## To start the CIFS server

### 1 To start the CIFS server, enter the following:

```
CIFS> server start
```

```
The skew of the system clock with respect to  
Domain controller is: -17 seconds
```

```
Time on Domain controller : Thu Dec 4 05:21:47 2008  
Time on this system : Thu Dec 4 05:22:04 PST 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
```

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

```
Enter password for user 'administrator':
```

**After you enter the correct password for the user administrator belonging to AD domain VERITASDOMAIN.COM, the following message appears:**

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

### 2 To make sure that the service is running, enter the following:

```
CIFS> server status
```

```
CIFS Status on test_01 : ONLINE  
CIFS Status on test_02 : ONLINE
```

```
Homedirfs           : fsl  
Security             : ads  
Domain membership status : Enabled  
Domain               : VERITASDOMAIN.COM  
Domain Controller    : VRTSSERVER  
Domain User          : administrator  
Clustering Mode      : normal
```

The CIFS server is now running in the AD domain mode. You can export the shares, and the domain users can access the shares subject to the AD authentication and authorization control.

## Using multi-domain controller support in CIFS

Veritas Access allows you to set a comma-separated list of primary and backup domain controllers for the given domain.

---

**Note:** You need to set dns nameserver for other domain controller (i.e. backup domain controller) using the `network dns set nameserver` command.

---

For example:

```
CIFS> set domaincontroller VRTSSERVER1,VRTSSERVER2,VRTSSERVER3
Global option updated. Note: Restart the CIFS server.
```

You will need to stop and start the CIFS server.

See [“Reconfiguring the CIFS service”](#) on page 198.

### To display the list of domain controllers

- ◆ To display the list of domain controllers, enter the following:

```
CIFS> show
Name                               Value
----                               -
netbios name                        access
ntlm auth                           yes
allow trusted domains               no
homedirfs
aio size                            1024
idmap backend rid                   10000-1000000
workgroup                           VERITASDOMAIN
security                            ads
Domain                              VERITASDOMAIN.COM
Domain user                          administrator
Domain Controller                   VRTSSERVER1 VRTSSERVER2 VRTSSERVER3
Clustering Mode                     normal
```

If the primary domain controller goes down, the CIFS server tries the next domain controller in the list until it receives a response. You should always point Veritas Access to the trusted domain controllers to avoid any security issues. Veritas Access does not perform list reduction or reordering, instead it uses the list as it is. So, avoid entering the redundant name for the same domain controller.

## About leaving an AD domain

There is no Veritas Access command that lets you leave an AD domain. It happens automatically as a part of change in security or domain settings, and then starts or stops the CIFS server. Thus, Veritas Access provides the domain leave operation depending on existing security and domain settings and new administrative commands. However, the leave operation requires the credentials of the old domain's user. All of the cases for a domain leave operation have been documented in [Table 11-2](#).

**Table 11-2** Change AD domain mode settings commands

Command	Definition
<code>set domain</code>	<p>Sets the domain.</p> <p>When you change any of the domain settings and you restart the CIFS server, the CIFS server leaves the old domain. Thus, when a change is made to either one or more of domain, domain controller, or domain user settings, and the next time the CIFS server is started, the CIFS server first attempts to leave the existing join and then joins the AD domain with the new settings.</p> <p>See <a href="#">"Changing domain settings for AD domain mode"</a> on page 171.</p>
<code>set security user</code>	<p>Sets the security user.</p> <p>If you change the security setting from <code>ads</code> to <code>user</code> and you stop or restart the CIFS server, it leaves the AD domain.</p> <p>When you change the security setting, and you stop or restart the CIFS server, the CIFS server leaves the existing AD domain. For example, the CIFS server leaves the existing AD domain if the existing security is <code>ads</code>, and the new security is changed to <code>user</code>, and the CIFS server is either stopped, or started again.</p> <p>See <a href="#">"Changing domain settings for AD domain mode"</a> on page 171.</p> <p>If the CIFS server is already stopped, changing the security to a value other than <code>ads</code> causes Veritas Access to leave the domain. Both the methods mentioned earlier require either stopping or starting the CIFS server. This method of leaving the domain is provided so that if a CIFS server is already stopped, and may not be restarted in near future, you should have some way of leaving an existing join to AD domain.</p> <p>See <a href="#">"Changing domain settings for AD domain mode"</a> on page 171.</p>

## Changing domain settings for AD domain mode

Each case assumes that the Veritas Access cluster is part of an AD domain.

### To verify the cluster is part of an AD domain

- ◆ To verify that the cluster is part of an AD domain, enter the following:

```
CIFS> server status
CIFS Status on access_01 : ONLINE
CIFS Status on access_02 : ONLINE

Homedirfs           : fs1
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Domain Controller   : VRTSSERVER
Domain User         : administrator
Clustering Mode     : normal
```

## To change domain settings for AD domain mode

- 1 To stop the CIFS server, enter the following:

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

- 2 To change the domain, enter the following:

```
CIFS> set domain newdomain.com
```

When you start the CIFS server, it tries to leave the existing domain. This requires the old domainuser to enter its password. After the password is supplied, and the domain leave operation succeeds, the CIFS server joins an AD domain with the new settings.

- 3 To start the CIFS server, enter the following:

```
CIFS> server start  
Disabling membership in existing AD domain VERITASDOMAIN.COM
```

```
Enter password for user 'administrator' of domain  
VERITASDOMAIN.COM :  
Left domain VERITASDOMAIN.COM
```

```
The skew of the system clock with respect to Domain controller is:  
-18 seconds
```

```
Time on this system: Thu Dec 4 05:21:47 2008  
Time on this system : Thu Dec 4 05:22:04 PST 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

```
Trying to become a member in AD domain NEWDOMAIN.COM...
```

```
Enter password for user 'administrator':
```

### To change the security settings for the AD domain mode

- ◆ To set the security to user, enter the following:

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

To stop the CIFS server:

```
CIFS> server stop
Disabling membership in existing AD domain VERITASDOMAIN.COM

Enter password for user 'administrator' of domain
VERITASDOMAIN.COM :
Stopping CIFS Server.....Success.
Left AD domain VERITASDOMAIN.COM
```

### Changing security settings with stopped server on the AD domain mode

- ◆ To set security to a value other than ads, enter the following:

```
CIFS> set security user
Disabling membership in existing AD domain VERITASDOMAIN.COM

Enter password for user 'administrator':
Left AD domain VERITASDOMAIN.COM
Global option updated. Note: Restart the CIFS server.
```

## Removing the AD interface

You can remove the Veritas Access cluster from the AD domain by using the Active Directory interface.

### To remove the Veritas Access cluster

- 1 Open the interface **Active Directory Users and Computers**.
- 2 In the domain hierarchy tree, click on **Computers**.
- 3 In the details pane, right-click the computer entry corresponding to Veritas Access (this can be identified by the Veritas Access cluster name) and click **Delete**.

## About setting NTLM

When you use Veritas Access in AD domain mode, there is an optional configuration step that can be done. You can disable the use of Microsoft NTLM (NT LAN Manager) protocol for authenticating users.

When the Veritas Access CIFS service is running in the standalone mode (with security set to user) some versions of the Windows clients require NTLM authentication to be enabled. You can do this by setting `CIFS> set ntlm_auth` to `yes`.

When NTLM is disabled and you use Veritas Access in AD domain mode, the available authentication protocols are Kerberos and NTLMv2. The one used depends on the capabilities of both the Veritas Access clients, and domain controller. If no special action is taken, Veritas Access allows the NTLM protocol to be used.

For any specific CIFS connection, all the participants, that is the client machine, Veritas Access and the domain controller select the protocol that they all support and that provides the highest security. In the AD domain mode, Kerberos provides the highest security.

## Setting NTLM

### To disable NTLM

- 1 If the server is running, enter the following:

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

- 2 To disable NTLM, enter the following:

```
CIFS> set ntlm_auth no
```

For example:

```
CIFS> set ntlm_auth no
Global option updated. Note: Restart the CIFS server.
```

- 3 To start the CIFS service, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

**To enable NTLM**

- 1 If the server is running, enter the following:

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

- 2 To enable the NTLM protocol, enter the following:

```
CIFS> set ntlm_auth yes
```

For example:

```
CIFS> set ntlm_auth yes
Global option updated. Note: Restart the CIFS server.
```

- 3 To start the CIFS service, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

## About setting trusted domains

The Microsoft Active Directory supports the concept of trusted domains. When you authenticate users, you can configure domain controllers in one domain to trust the domain controllers in another domain. This establishes the trust relation between the two domains. When Veritas Access is a member in an AD domain, both Veritas Access and the domain controller are involved in authenticating the clients. You can configure Veritas Access to support or not support trusted domains.

**Table 11-3** Set trusted domains commands

Command	Definition
<pre>set allow_trusted_domains yes</pre>	<p>Enables the use of trusted domains in the AD domain mode.</p> <p><b>Note:</b> If the security mode is <code>user</code>, it is not possible to enable AD trusted domains. All the IDMAP backend methods (<code>rid</code>, <code>ldap</code>, and <code>hash</code>) are able to support trusted domains.</p> <p>See <a href="#">“Setting Active Directory trusted domains”</a> on page 192.</p>
<pre>set allow_trusted_domains no</pre>	<p>Disables the use of trusted domains in the AD domain mode.</p> <p>See <a href="#">“Setting Active Directory trusted domains”</a> on page 192.</p>

## Specifying trusted domains that are allowed access to the CIFS server

You can specify the trusted domains that are allowed access to a CIFS server when the `CIFS> set allow_trusted_domains` option is set to `yes`, and `idmap_backend` is set to `rid` or `ad`.

See [“Allowing trusted domains access to CIFS when setting an IDMAP backend to rid”](#) on page 178.

By default, all the trusted domains of the joined active directory domain are included in the CIFS settings and configuration if `allow_trusted_domains` is set to `yes`.

By default, `CIFS> set allow_trusted_domains` is set to `no`.

### To specify the trusted domains that are allowed access to the CIFS server

- ◆ To specify the trusted domains that are allowed access to the CIFS server, enter the following:

```
CIFS> set allow_trusted_domains yes | no [trusted_domains]
```

where *trusted\_domains* are the trusted domains that you want to allow access to the CIFS server.

## Allowing trusted domains access to CIFS when setting an IDMAP backend to rid

### To allow trusted domains access to CIFS when setting IDMAP backend to rid

- 1 If the CIFS server is running, enter the following:

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

- 2 To set the `idmap_backend` to `rid`, enter the following:

```
CIFS> set idmap_backend rid [uid_range]
```

where *uid\_range* represents the range of identifiers that are used by Veritas Access when mapping domain users and groups to local users and groups.

You can obtain unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions. This is a read-only idmap backend. Trusted domains are allowed if `set allow_trusted_domains` is set to `yes`. A valid user from a domain or trusted domain should have a UID as well as a GID for the user's primary group.

By default, the *uid\_range* is set to 10000-1000000. Change it in cases where there are more than 1,000,000 users existing on a local Veritas Access cluster where there are joined Active Directory domains or trusted domains.

---

**Note:** The *uid\_range* is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

---

```
CIFS> set idmap_backend rid  
Global option updated. Note: Restart the CIFS server.
```

- 3 To set `allow_trusted_domains` to `yes`, enter the following:

```
CIFS> set allow_trusted_domains yes  
Global option updated. Note: Restart the CIFS server.
```

- 4 To start the CIFS server again, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

- 5 To verify the CIFS server status when there are trusted domains, enter the following:

```
CIFS> server status  
CIFS Status on test_01      : ONLINE  
CIFS Status on test_02      : ONLINE  
  
Homedirfs                   : homefs  
Security                     : ads  
Domain membership status    : Enabled  
Domain                       : VERITASDOMAIN.COM  
Workgroup                    : VERITASDOMAIN  
Domain Controller           : VRTSSERVER  
Domain User                  : administrator  
Clustering Mode             : normal  
Trusted Domains             : VERITASDOMAIN1 [VERITASDOMAIN2]  
VERITASDOMAIN3
```

Domain names containing square brackets indicate that the domain used to be a trusted domain, but the domain is currently obsolete.

## Allowing trusted domains access to CIFS when setting an IDMAP backend to ldap

### To allow trusted domains access to CIFS when setting an IDMAP backend to ldap

- 1 To configure AD as an IDMAP backend, follow the steps provided at:

See [“About configuring Windows Active Directory as an IDMAP backend for CIFS”](#) on page 185.

- 2 To set `idmap_backend` to `ldap`, enter the following:

```
CIFS> set idmap_backend ldap [idmap_ou] [uid_range]
```

`idmap_ou` Specifies the CIFS idmap Organizational Unit Name (OU) configured on the LDAP server, which is used by Veritas Access when mapping users and groups to local users and groups. The default value is `cifsidmap`.

`uid_range` Specifies the range of identifiers that are used by Veritas Access when mapping domain users and groups to local users and groups.

You can obtain unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions. This is a read-only idmap backend. Trusted domains are allowed if `set allow_trusted_domains` is set to `yes`. A valid user from a domain or trusted domain should have a UID as well as a GID for the user's primary group.

By default, the `uid_range` is set to 10000-1000000. Change it in cases where there are more than 1,000,000 users existing on a local Veritas Access cluster where there are joined Active Directory domains or trusted domains.

**Note:** The `uid_range` is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

```
CIFS> set idmap_backend ldap
```

Global option updated. Note: Restart the CIFS server.

- 3 To set `allow_trusted_domains` to `yes`, enter the following:

```
CIFS> set allow_trusted_domains yes
```

Global option updated. Note: Restart the CIFS server.

- 4 To restart the CIFS server again, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

- 5 To verify the CIFS server status when there are trusted domains, enter the following:

```
CIFS> server status  
CIFS Status on test_01      : ONLINE  
CIFS Status on test_02      : ONLINE  
  
Homedirfs                   : homefs  
Security                     : ads  
Domain membership status    : Enabled  
Domain                       : VERITASDOMAIN.COM  
Workgroup                    : VERITASDOMAIN  
Domain Controller           : VRTSSERVER  
Domain User                  : administrator  
Clustering Mode             : normal  
Trusted Domains             : VERITASDOMAIN1 VERITASDOMAIN2  
VERITASDOMAIN3
```

## Allowing trusted domains access to CIFS when setting an IDMAP backend to hash

### To allow trusted domains access to CIFS when setting an IDMAP backend to hash

- 1 If the CIFS server is running, enter the following:

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

- 2 To set `idmap_backend` to `hash`, enter the following:

```
CIFS> set idmap_backend hash  
Global option updated. Note: Restart the CIFS server.
```

You can obtain unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions. This is a read-only idmap backend. Trusted domains are allowed if `set allow_trusted_domains` is set to `yes`. A valid user from a domain or trusted domain should have a UID as well as a GID for the user's primary group.

By default, the `uid_range` is set to 10000-1000000. Change it in cases where there are more than 1,000,000 users existing on a local Veritas Access cluster where there are joined Active Directory domains or trusted domains.

---

**Note:** The `uid_range` is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

---

**3** To set `allow_trusted_domains` to `yes`, enter the following:

```
CIFS> set allow_trusted_domains yes
```

Global option updated. Note: Restart the CIFS server.

**4** To verify the CIFS server status when there are trusted domains, enter the following:

```
CIFS> server status
```

```
CIFS Status on test_01      : ONLINE
```

```
CIFS Status on test_02      : ONLINE
```

```
Homedirfs                  : homefs
```

```
Security                    : ads
```

```
Domain membership status   : Enabled
```

```
Domain                      : VERITASDOMAIN.COM
```

```
Workgroup                   : VERITASDOMAIN
```

```
Domain Controller           : VRTSSERVER
```

```
Domain User                  : administrator
```

```
Clustering Mode             : normal
```

```
Trusted Domains              : VERITASDOMAIN1 VERITASDOMAIN2
```

```
VERITASDOMAIN3
```

## Allowing trusted domains access to CIFS when setting an IDMAP backend to ad

### To allow trusted domains access to CIFS when setting IDMAP backend to ad

- 1 If the CIFS server is running, enter the following:

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

- 2 To set the `idmap_backend` to `ad`, enter the following:

```
CIFS> set idmap_backend ad [uid_range]
```

where `uid_range` represents the range of identifiers that are used by Veritas Access when mapping domain users and groups to local users and groups.

You can obtain unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions. This is a read-only `idmap` backend. Trusted domains are allowed if `set allow_trusted_domains` is set to `yes`. A valid user from a domain or trusted domain should have a UID as well as a GID for the user's primary group.

By default, the `uid_range` is set to 10000-1000000. Change it in cases where there are more than 1,000,000 users existing on a local `&product_name_isa;` cluster where there are joined Active Directory domains or trusted domains.

---

**Note:** The `uid_range` is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

---

- 3 To set `allow_trusted_domains` to `yes`, enter the following:

```
CIFS> set allow_trusted_domains yes  
Global option updated. Note: Restart the CIFS server.
```

- 4 To start the CIFS server again, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

- 5 To verify the CIFS server status when there are trusted domains, enter the following:

```
CIFS> server status  
CIFS Status on test_01      : ONLINE  
CIFS Status on test_02      : ONLINE  
  
Homedirfs                  : homefs  
Security                   : ads  
Domain membership status   : Enabled  
Domain                     : VERITASDOMAIN.COM  
Workgroup                  : VERITASDOMAIN  
Domain Controller         : VRTSSERVER  
Domain User                : administrator  
Clustering Mode           : normal  
Trusted Domains           : VERITASDOMAIN1 [VERITASDOMAIN2]  
VERITASDOMAIN3
```

Domain names containing square brackets indicate that the domain used to be a trusted domain, but the domain is currently obsolete.

## About configuring Windows Active Directory as an IDMAP backend for CIFS

The CIFS server requires equivalent UNIX identities for Windows accounts to service requests from Windows clients. In the case of trusted domains, Veritas Access has to store the mapped UNIX identities (IDMAP) in a centralized database that is accessible from each of the cluster nodes.

Active Directory (AD), as with any LDAP V3 compliant directory service, can function as the backend for CIFS IDMAP backend storage. When the CIFS server joins a Windows Active Directory Domain as a member server, and you want to use LDAP as an IDMAP backend, then it is necessary to create an Active Directory application partition for the IDMAP database. To support the creation of an Active Directory application partition, Windows 2003 R2 and above version is required.

Active Directory application partition provides the ability to control the scope of replication and allow the placement of replicas in a manner more suitable for dynamic data. As a result, the application directory partition provides the capability of hosting dynamic data in the Active Directory server, thus allowing ADSI/LDAP access to it.

By extending the AD schema with the necessary CIFS-schema extensions, and creating an AD application partition, it is possible to store CIFS IDMAP data entries in AD, using one or more domain controllers as IDMAP LDAP backend servers. Also, it is possible to replicate this information in a simple and controlled manner to a subset of AD domain controllers located either in the same domain or in different domains in the AD forest.

---

**Note:** A single domain user account is used, for example, **cifsuser** for setting application partition Access Control List (ACL) settings. Make sure the selected user naming context has no space key inside (for example, **CN=cifsuser1,CN=Users,DC=example,DC=com**). A sample AD server is used, for example, **adserver.example.com**. Use relevant values when configuring your AD server.

---

## Configuring the Active Directory schema with CIFS-schema extensions

### To extend the Active Directory schema with the necessary CIFS-schema extensions

- 1 Login with **Schema Admins** privileges on the Active Directory Forest Schema Master domain controller.
- 2 Download `ADCIFSSchema.zip` from the Veritas Access server (`/opt/SYMCsnas/install/ADCIFSSchema.zip`) with software such as `WinSCP.exe`.
- 3 Unzip the file and open each `.ldf` file to perform a search and replace of the string `dc=example,dc=com`, replacing the string with the top-level domain component (that is, `dc=yourdomain,dc=com`) values for the AD forest.
- 4 Install the schema extensions by executing the `schemaupdate.bat` file from the command prompt.

### To validate the schema extensions

- 1 Execute `regsvr32 schmmgmt.dll` in a command prompt window to install the Active Directory Schema Snap-In on the AD server.
- 2 Enter `mmc` in **Run**.
- 3 On the **File** menu, click **Add/Remove Snapin**.
- 4 In **Available snap-ins**, click **Active Directory Schema**, and then click **Add**.

- 5 Click **OK**.
- 6 Click **Attributes** in the left frame, and try to find **uidNumber** and **gidNumber** in the right frame.

Validate that the **uidNumber** and **gidNumber** attributes have no minimum or maximum value setting by viewing the properties of the attribute objects.

### To create an application partition

- 1 Open a command prompt window on the domain controller that will hold the first replica of the application partition.
- 2 Enter `ntdsutil` in the command prompt window.
- 3 At the `ntdsutil` command prompt, enter the following:

```
domain management
```

If you are using Windows 2008, change this command to the following:

```
partition management
```

- 4 At the domain management command prompt, enter the following:

```
connection
```

- 5 At the connection command prompt, enter the following:

```
connect to server adserver.example.com
```

- 6 At the connection command prompt, enter the following:

```
quit
```

- 7** At the domain management command prompt, enter the following such as:

```
create nc dc=idmap,dc=example,dc=com null
```

**Example settings:**

```
C:\>ntdsutil
ntdsutil: domain management
domain management: connection
server connections: connect to server adserver.example.com
Binding to adserver.example.com ...
Connected to adserver.si2m.com using credentials of locally logged
on user.
server connections: quit
domain management: create nc dc=idmap,dc=example,dc=com NULL
adding object dc=idmap,dc=example,dc=com
domain management: quit
ntdsutil: quit
Disconnecting from adserver.example.com...
```

- 8 Once the application partition has been created, open **ADSIedit.msc** from **Run**, then right-click on **ADSI Edit** in the left frame, and click **connect to ...** to connect to the application partition using the settings as indicated:

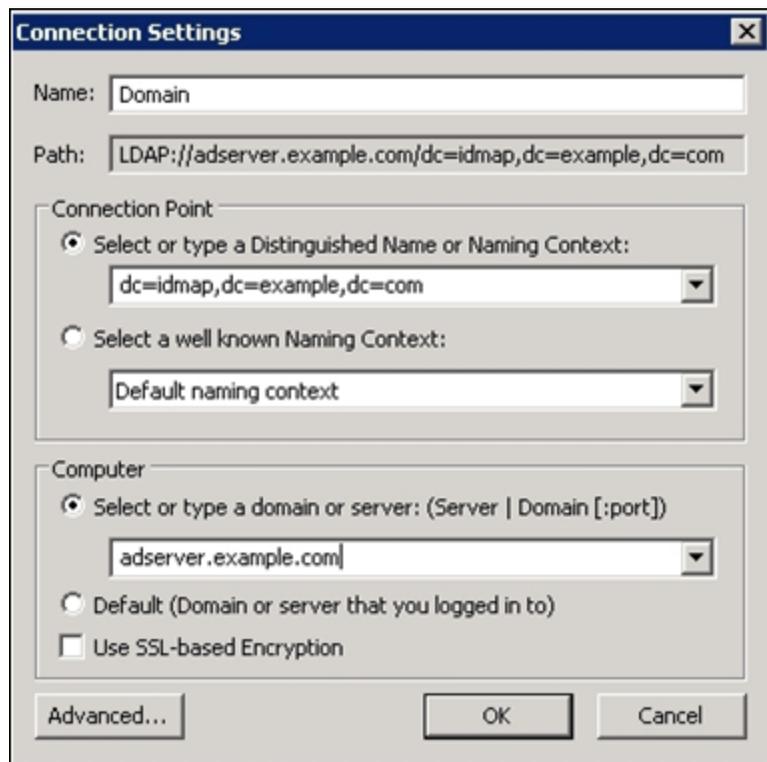
Name Enter **Domain**.

Connection Point Select or enter a **Distinguished Name** or **Naming Context**, as in:

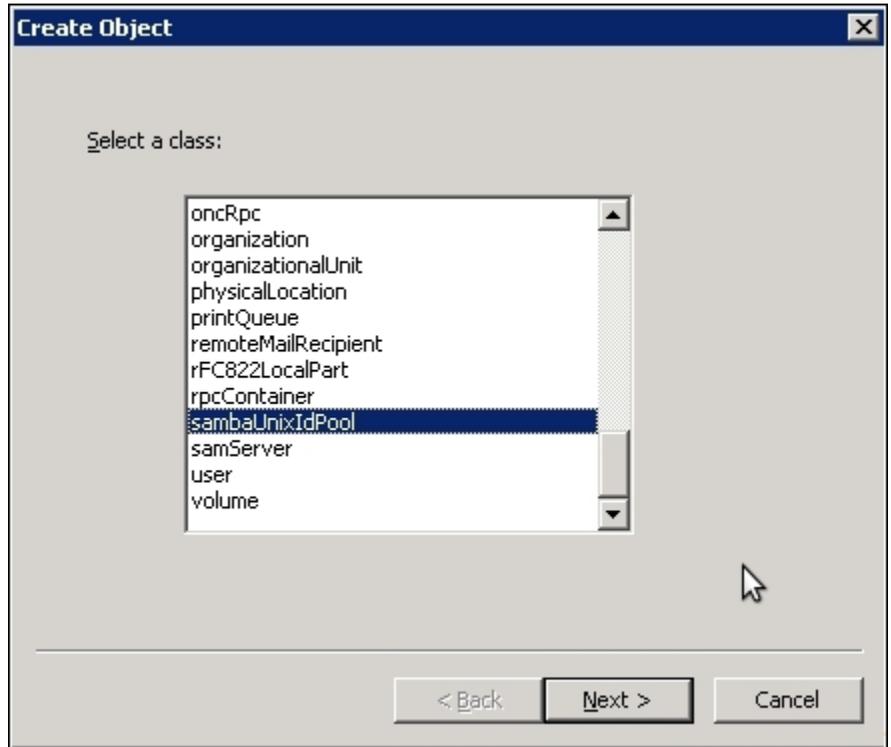
dc=idmap,dc=example,dc=com

Computer Select or enter a domain or server, as in:

adserver.example.com



- 9 Once connected, select the top-level application partition (for example, **dc=idmap,dc=example,dc=com**) node in the left panel, and right-click to select **New** then **Object** from the list, and then select **SambaUnixIdPool**.



When prompted, enter the following values:

OU attribute	<b>cifsidmap</b>
uidNumber	<b>10000</b>
gidNumber	<b>10000</b>

- 10 Click **Finish** to complete the configuration.
- 11 Once the **ou=cifsidmap,dc=idmap,dc=example,dc=com** container has been created, right-click the object, and select **properties**.
- 12 On the **Security** tab, click **Add**, and proceed to add the cifsuser user account, and grant the account Read, Write, Create All Child Objects, and Delete All Child Objects permissions.

## Configuring the LDAP client for authentication using the CLI

### To configure the LDAP client for authentication using the CLI

- 1 Log into the cluster CLI using the `master` account.
- 2 Configure `Network> ldap` settings.

Example settings:

```
Network> ldap set basedn dc=idmap,dc=example,dc=com
Network> ldap set binddn cn=cifsuser,dc=example,dc=com
Network> ldap set rootbinddn cn=cifsuser,cn=users,dc=example,dc=com
Network> ldap set server adserver.example.com
Network> ldap enable
```

## Configuring the CIFS server with the LDAP backend

### To configure the CIFS server with the LDAP backend

- 1 Log in to the Veritas Access cluster CLI using the `master` account.
- 2 Set the domain, domaincontroller, and domainuser.
- 3 Set security to `ads`.

- 4 Set `idmap_backend` to `ldap`, and specify `idmap OU` as `cifsidmap`.

Example settings:

```
CIFS> set domain example.com
CIFS> set domainuser administrator
CIFS> set domaincontroller adserver.example.com
CIFS> set security ads
CIFS> set idmap_backend ldap cifsidmap
CIFS> server start
```

- 5 Start the CIFS server.

The CIFS server will take some time to import all the users from the joined domain and trusted domain(s) to the application partition. Wait for at least ten minutes before trying to access the shares from Windows clients after starting the CIFS server.

To validate that IDMAP entries are being entered correctly in the Active Directory application partition, connect to the Active Directory application partition using an LDAP administration tool, for example, LDP or ADSIEdit. Expand the IDMAP container (`ou=cifsidmap`). There should be numerous entries.

## Setting Active Directory trusted domains

### To enable Active Directory (AD) trusted domains

- 1 If the server is running, enter the following:

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

- 2 To enable trusted domains, enter the following:

```
CIFS> set allow_trusted_domains yes
```

For example:

```
CIFS> set allow_trusted_domains yes
Global option updated. Note: Restart the CIFS server.
```

- 3 To start the CIFS server, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

### To disable trusted domains

- 1 If the server is running, enter the following:

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

- 2 To disable trusted domains, enter the following:

```
CIFS> set allow_trusted_domains no
```

For example:

```
CIFS> set allow_trusted_domains no
Global option updated. Note: Restart the CIFS server.
```

- 3 To start the CIFS server, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

## About storing account information

Veritas Access maps between the domain users and groups (their identifiers) and local representation of these users and groups. Information about these mappings can be stored locally on Veritas Access or remotely using the DC directory service. Veritas Access uses the `idmap_backend` configuration option to decide where this information is stored.

This option can be set to one of the following:

<code>rid</code>	Maps SIDs for domain users and groups by deriving UID and GID from RID on the Veritas Access CIFS server.
<code>ldap</code>	Stores the user and group information in the LDAP directory service.
<code>hash</code>	Maps SIDs for domain users and groups to 31-bit UID and GID by the implemented hashing algorithm on the Veritas Access CIFS server.
<code>ad</code>	Obtains unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions.

---

**Note:** SID/RID are Microsoft Windows concepts that can be found at:  
[http://msdn.microsoft.com/en-us/library/aa379602\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa379602(VS.85).aspx).

---

The `rid` and `hash` values can be used in any of the following modes of operation:

- Standalone
- AD domain

`rid` is the default value for `idmap_backend` in all of these operational modes. The `ldap` value can be used if the AD domain mode is used.

When security is set as "user" `idmap_backend` is irrelevant.

**Table 11-4** Store account information commands

Command	Definition
<pre>set idmap_backend rid</pre>	<p>Configures Veritas Access to store information about users and groups locally.</p> <p>Trusted domains are allowed if <code>allow_trusted_domains</code> is set to <code>yes</code>. The <code>uid_range</code> is set to 10000-1000000 by default.</p> <p>Change the default range in cases where it is not appropriate to accommodate local Veritas Access cluster users, Active Directory, or trusted domain users.</p> <p>Do not attempt to modify <code>LOW_RANGE_ID</code> (10000) if user data has already been created or copied on the CIFS server. This may lead to data access denied issues since the UID changes.</p> <p>See <a href="#">"Storing user and group accounts"</a> on page 195.</p>
<pre>set idmap_backend hash</pre>	<p>Allows you to obtain the unique SID to UID/GID mappings by the implemented hashing algorithm. Trusted domains are allowed if <code>allow_trusted_domains</code> is set to <code>yes</code>.</p> <p>See <a href="#">"Storing user and group accounts"</a> on page 195.</p>
<pre>set idmap_backend ad</pre>	<p>Allows you to obtain unique user IDs (UIDs) or group IDs (GIDs) from domains by reading ID mappings from an Active Directory server that uses RFC2307/SFU schema extensions.</p> <p>See <a href="#">"Storing user and group accounts"</a> on page 195.</p>

**Table 11-4** Store account information commands (*continued*)

Command	Definition
set idmap_backend ldap	<p>Configures Veritas Access to store information about users and groups in a remote LDAP service. You can only use this command when Veritas Access is operating in the AD domain mode. The LDAP service can run on the domain controller or it can be external to the domain controller.</p> <p><b>Note:</b> For Veritas Access to use the LDAP service, the LDAP service must include both RFC 2307 and proper schema extensions.</p> <p>See <a href="#">“Configuring the LDAP client for authentication using the CLI”</a> on page 191.</p> <p>This option tells the CIFS server to obtain SID to UID/GID mappings from a common LDAP backend. This option is compatible with multiple domain environments. So <code>allow_trusted_domains</code> can be set to <code>yes</code>.</p> <p>If <code>idmap_backend</code> is set to <code>ldap</code>, you must first configure the Veritas Access LDAP options using the <code>Network&gt; ldap</code> commands.</p> <p>See <a href="#">“About configuring LDAP settings”</a> on page 74.</p> <p>See <a href="#">“Storing user and group accounts”</a> on page 195.</p>

## Storing user and group accounts

### To set `idmap_backend` to `rid`

- 1 If the server is running, enter the following:

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

- 2 To store information about user and group accounts locally, enter the following:

```
CIFS> set idmap_backend rid [uid_range]
```

where `uid_range` represents the range of identifiers that are used by Veritas Access when mapping domain users and groups to local users and groups. The default range is `10000-1000000`.

- 3 To start the CIFS server, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

### To set `idmap_backend` to LDAP

- 1 To make sure that you have first configured LDAP, enter the following:

```
Network> ldap show
```

- 2 If the CIFS server is running, enter the following:

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

- 3 To use the remote LDAP store for information about the user and group accounts, enter the following:

```
CIFS> set idmap_backend ldap [idmap_ou]
```

where *idmap\_ou* represents the CIFS idmap Organizational Unit Name (OU) configured on the LDAP server, which is used by Veritas Access when mapping users and groups to local users and groups. The default value is `cifsidmap`.

- 4 To start the CIFS server, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

### To set `idmap_backend` to a hash algorithm

- 1 If the CIFS server is running, enter the following:

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

- 2 To store information about user and group accounts locally, enter the following:

```
CIFS> set idmap_backend hash
```

- 3 To start the CIFS server, enter the following:

```
CIFS> server start  
Starting CIFS Server.....Success.
```

### To set `idmap_backend` to `ad`

- 1 If the CIFS server is running, enter the following:

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

- 2 To obtain the unique UID/GID from domains by reading ID mappings from an Active Directory (AD) server, enter the following:

```
CIFS> set idmap_backend ad [uid_range]
```

where `uid_range` represents the range of identifiers that are used by Veritas Access when mapping domain users and groups to local users and groups. The default range is `10000-1000000`. Change it in cases where there are more than 1,000,000 users existing on a local Veritas Access cluster where there are joined Active Directory domains or trusted domains.

---

**Note:** The `uid_range` is adjusted automatically according to the search results of the defined UNIX IDs from the domain after a CIFS server restart.

---

- 3 To start the CIFS server, enter the following:

```
CIFS> server start
Starting CIFS Server.....Success.
```

## About reconfiguring the CIFS service

Sometime after you have configured the CIFS service, and used it for awhile, you need to change some of the settings. For example, you may want to allow the use of trusted domains or you need to move Veritas Access from one security domain to another. To carry out these changes, set the new settings and then start the CIFS server. As a general rule, you should stop the CIFS service before making the changes.

An example where Veritas Access is moved to a new security domain (while the mode of operation stays unchanged as, AD domain) is referenced in the section below.

See [“Reconfiguring the CIFS service”](#) on page 198.

This example deals with reconfiguring CIFS. So make sure that if any of the other AD services like DNS or NTP are being used by Veritas Access, that Veritas Access

has already been configured to use these services from the AD server belonging to the new domain.

Make sure that the DNS service, NTP service and, if used as an ID mapping store, also the LDAP service, are configured as required for the new domain.

To reconfigure the CIFS service, do the following:

- Make sure that the server is not running.
- Set the domain user, domain, and domain controller.
- Start the CIFS server.

## Reconfiguring the CIFS service

### To set the user name for the AD

- 1 To verify that the CIFS server is stopped, enter the following:

```
CIFS> server status
```

- 2 If the server is running, stop the server, and enter the following:

```
CIFS> server stop
```

- 3 To set the user name for the AD, enter the following:

```
CIFS> set domainuser username
```

where *username* is the name of an existing AD domain user who has permission to perform the join domain operation.

For example:

```
CIFS> set domainuser administrator
```

```
Global option updated. Note: Restart the CIFS server.
```

### To set the AD domain

- ◆ To set the AD domain, enter the following:

```
CIFS> set domain domainname
```

where *domainname* is the name of the domain. This command also sets the system workgroup. For example:

```
CIFS> set domain NEWDOMAIN.COM
```

```
Global option updated. Note: Restart the CIFS server.
```

**To set the AD server**

- ◆ To set the AD server, enter the following:

```
CIFS> set domaincontroller servername
```

where *servername* is the AD server IP address or DNS name.

For example, if the AD server VRTSSERVER has an IP address of 172.16.113.118, you can specify one of the following:

```
CIFS> set domaincontroller 172.16.113.118
```

Global option updated. Note: Restart the CIFS server.

Or

```
CIFS> set domaincontroller SYMSERVER
```

Global option updated. Note: Restart the CIFS server.

If you use the AD server name, you must configure Veritas Access to use a DNS server that can resolve this name.

### To start the CIFS server

- 1 To start the CIFS server, enter the following:

```
CIFS> server start
```

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

```
Time on Domain controller : Fri May 30 06:00:03 2008  
Time on this system : Fri May 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..
```

- 2 To make sure that the service is running, enter the following:

```
CIFS> server status
```

- 3 To find the current settings, enter the following:

```
CIFS> show
```

## About mapping user names for CIFS/NFS sharing

The CIFS server uses user name mapping to translate login names sent by a Windows client to local or remote UNIX user names. The CIFS server uses file lookup for mapping, and this mapping is unidirectional. You can map a CIFS user to an NFS user, but the reverse operation is not possible.

This functionality can be used for the following purposes:

- CIFS and NFS sharing by mapping CIFS users to NFS users
- File sharing among CIFS users by mapping multiple CIFS users to a single UNIX user

- Mapping between two UNIX users by using the `CIFS> mapuser add <CIFSusername> LOCAL <NFSusername>` command, where both the CIFS user and the NFS user are UNIX users

User name mapping is stored in a configuration file.

When user name mapping takes place is dependent on the current security configurations. If security is set to `user`, mapping is done prior to authentication, and a password must be provided for the mapped user name. For example, if there is a mapping between the users `CIFSuser1` and `NFSuser1`. If `CIFSuser1` wants to connect to the Veritas Access server, then `CIFSuser1` needs to provide a password for `NFSuser1`. In this case, `NFSuser1` must be the CIFS local user.

If security is set to either `ads` or `domain`, user name mapping is done after authentication with the domain controller. This means, the actual password must be supplied for the login user `CIFSuser1` in the example cited above. In this case, `NFSuser1` may not be the CIFS local user.

For example, to map a CIFS user to an NFS user:

```
CIFS> mapuser add CIFSuser1 VERITASDOMAIN.COM NFSuser1
```

For example, to show the mapping between a CIFS user and an NFS user:

```
CIFS> mapuser show
CIFSUserName DomainName NFSUserName
CIFSuser1 VERITASDOMAIN NFSuser1
```

For example, to remove the mapping between a CIFS user and an NFS user:

```
CIFS> mapuser remove CIFSuser1 VERITASDOMAIN.COM
```

The domain you specify for CIFS user name mapping must be the netbios domain name (instead of the Active Directory DNS domain name) for the user. For example, a netbios domain name might be listed as `VERITASDOMAIN` instead of `VERITASDOMAIN.COM` (without the `.com` extension).

To determine the netbios domain name, login to your Active Directory Server and type the following in a command window:

```
set | findstr DOMAIN
```

The results will include:

```
USERDOMAIN netbios_domain_name
USERDNSDOMAIN Active_Directory_DNS_domain_name
```

Use the value of `USERDOMAIN` (the netbios domain name) when you map user names.

---

**Note:** When setting quotas on home directories and using user name mapping, make sure to set the quota on the home directory using the user name to which the original name is mapped.

---

---

**Note:** For mapped Active Directory users to access their home directory CIFS shares, use the following convention: `\\access\realADuser` instead of `\\access\homes`.

---

---

**Note:** For UNIX users (LDAP/NIS/local) users, make sure to set up these users properly, so that these users are recognized by Samba. User mapping can work properly only after these users are recognized by Samba.

See [“Configuring the CIFS server with the LDAP backend”](#) on page 191.

---

## About the mapuser commands

The `CIFS> mapuser` commands are used to add, remove, or display the mapping between CIFS and NFS users.

Typically, a *CIFSusername* is a user coming from an AD server (with a specified domainname), or a locally created CIFS user on this system (local). An *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.

---

**Note:** To make sure user mappings work correctly with a NIS/LDAP server, `Network> nsswitch` settings may need to be adjusted in the `Network> nsswitch` section. You may need to move the position of `ldap` or `nis` in the `Network> nsswitch` section, depending on which name service is being used first.

---

# Adding, removing, or displaying the mapping between CIFS and NFS users

## To add a mapping between a CIFS and an NFS user

- ◆ To add a mapping between a CIFS and an NFS user, enter the following:

```
CIFS> mapuser add CIFSusername domainname NFSusername
```

For example, to map a CIFS user to an NFS user:

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

For example, to add a mapping between all the same name users between CIFS and NFS:

```
CIFS> mapuser add * VERITASDOMAIN.COM *
```

## To remove a mapping between a CIFS and an NFS user

- ◆ To remove a mapping between a CIFS and an NFS user, enter the following:

```
CIFS> mapuser remove CIFSusername [domainname]
```

For example, to remove a mapping between a CIFS and an NFS user:

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

For example, to remove a mapping between the same name user for a CIFS and an NFS user:

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

## To display a mapping between a CIFS and an NFS user

- ◆ To display a mapping between a CIFS and an NFS user, enter the following:

```
CIFS> mapuser show [CIFSusername] [domainname]
```

For example, to display the mapping between a CIFS and an NFS user:

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

```
CIFSUserName      DomainName        NFSUserName
administrator      VERITASDOMAIN    nfsusr1
```

# Automatically mapping of UNIX users from LDAP to Windows users

## To automatically map UNIX users from LDAP to Windows users

- 1 Ensure that Veritas Access joins the LDAP domain using **network ldap**.

From the LDAP server, users and groups should be visible by using the `getent passwd` or `getent group` commands.

- 2 Ensure that Veritas Access joins the Windows AD domain using **cifs**.

- 3 Use the wildcard mapping rule `CIFS> mapuser add * AD Domain Name *`.

The effect is whenever a Windows domain user, say `DOM\foobar`, wants to access CIFS shares, the CIFS server determines if there is a local (a non-Windows) user also named `foobar`, and establishes the mapping between the Windows user and the non-Windows user.

The user name must match between the LDAP and AD domains.

## About managing home directories

You can use Veritas Access to store the home directories of CIFS users.

The home directory share name is identical to the Veritas Access user name. When Veritas Access receives a new CIFS connection request, it checks if the requested share is one of the ordinary exported shares. If it is not, Veritas Access checks if the requested share name is the name of an existing Veritas Access user (either local user or domain user, depending on the current mode of operation). If a match is found, it means that the received connection request is for a home directory share.

You can access your home directory share the same way you access the file system ordinary shares. A user can connect only to his or her own home directory.

---

**Note:** The internal directories structure of home directory file systems is maintained by Veritas Access. It is recommended not to use a file system as a `homedirfs` that has been used by a normal share in the past or vice versa.

---

## Setting the home directory file systems

Home directory shares are stored in one or more file systems. A single home directory can exist only in one of these file systems, but a number of home directories

can exist in a single home directory file system. File systems that are to be used for home directories are specified using the `CIFS> set homedirfs` command.

When a file system is exported as a homedirfs, its mode is set to a 0755 value. This takes place when you start the CIFS server after setting the homedirfs list.

---

**Note:** Snapshots cannot be shared as home directory file systems.

---

### To specify one or more file systems as the home directories

- 1 To reserve one or more file systems for home directories, enter the following:

```
CIFS> set homedirfs [filesystemlist]
```

where *filesystemlist* is a comma-separated list of names of the file systems which are used for the home directories.

For example:

```
CIFS> set homedirfs fs1,fs2,fs3
```

Global option updated. Note: Restart the CIFS server.

- 2 If you want to remove the file systems you previously set up, enter the command again, without any file systems:

```
CIFS> set homedirfs
```

- 3 To find which file systems (if any) are currently used for home directories, enter the following:

```
CIFS> show
```

After you select one or more of the file systems to be used in this way, you cannot export the same file systems as ordinary CIFS shares.

If you want to change the current selection, for example, to add an additional file system to the list of home directory file systems or to specify that no file system should be used for home directories, you have to use the same `CIFS> set homedirfs` command. In each case you must enter the entire new list of home directory file systems, which may be an empty list when no home directory file systems are required.

Veritas Access treats home directories differently from ordinary shares. The differences are as follows:

- An ordinary share is used to export a file system, while a number of home directories can be stored in a single file system.

- The file systems used for home directories cannot be exported as ordinary shares.
- Exporting a home directory share is done differently than exporting an ordinary share. Also, removing these two kinds of shares is done differently.
- The configuration options you specify for an ordinary share (such as read-only or use of opportunistic locks) are different from the ones you specify for a home directory share.

## Setting up home directories

You can set the home directory for the specified user with the `CIFS> homedir set` command. If the home directory does not exist for the specified user, the `CIFS> homedir set` command creates that user's home directory.

Use the `Storage> quota cifshomedir set` command to set the quota value for the specified user. Otherwise, the value set from the `Storage> quota cifshomedir setdefault` command is used to configure the quota limit. If either the user or default quota is not set, 0 is used as the default value for the unlimited quota.

Once the global quota value is specified, the value applies to the automatically created homedir. For example, if you set the global quota value to `Storage> quota cifshomedir setdefault 100M`, and you then create a new homedir in Windows, then the 100M quota value is assigned to that homedir.

## To set the home directory for the specified user

- 1 To set the home directory for the specified user, enter the following:

```
CIFS> homedir set username [domainname] [fsname]
```

*username* The name of the CIFS user. If a CIFS user name includes a space, enter the user name with double quotes.

For example:

```
CIFS> homedir set "test user" VERITASDOMAIN
```

*domainname* The domain for the new home directory.

*fsname* The home directory file system where the user's home directory is created. If no file system is specified, the user's home directory is created on the home directory file system that has the fewest home directories.

- 2 To find the current settings for a home directory, enter the following:

```
CIFS> homedir show [username] [domainname]
```

*username* The name of the CIFS user. If a CIFS user name includes a space, enter the user name with double quotes.

For example:

```
CIFS> homedir show "test user" VERITASDOMAIN
UserName      DomainName    Usage
test user    VERITASDOMAIN 0
```

*domainname* The Active Directory/Windows NT domain name or specify `local` for the Veritas Access local user `local`.

- 3 To find the current settings for all home directories, enter the following:

```
CIFS> homedir show
```

Because the `CIFS> homedir show` command takes a long time when there are more than 1000 CIFS home directories to display, you will be prompted if you want to continue displaying CIFS home directories or not.

When you connect to your home directory for the first time, and if the home directory has not already been created, Veritas Access selects one of the available home directory file systems and creates the home directory there. The file system is selected in a way that tries to keep the number of home directories balanced across all available home directory file systems. The automatic creation of a home directory does not require any commands, and is transparent to both the users and the Veritas Access administrators.

The quota limits the amount of disk space you can allocate for the files in a home directory.

You can set the same quota value for all home directories using the `Storage> quota cifshomedir setall` command.

See [“Using quotas for CIFS home directories”](#) on page 370.

## Displaying home directory usage information

You can display information about home directories using the `CIFS> homedir show` command.

---

**Note:** Information about home directory quotas is up-to-date only when you enable the use of quotas for the home directory file systems.

---

## To display information about home directories

- 1 To display information about a specific user's home directory, enter the following:

```
CIFS> homedir show [username] [domainname]
```

*username* The name of the CIFS user. If a CIFS user name includes a space, enter the user name with double quotes.

For example:

```
CIFS> homedir show "test user" VERITASDOMAIN
UserName  DomainName      Filesystem Usage
test user VERITASDOMAIN /vx/fs3      0
```

*domainname* The domain where the home directory is located.

- 2 To display information about all home directories, enter the following:

```
CIFS> homedir show
```

## Deleting home directories and disabling creation of home directories

You can delete a home directory share. This also deletes the files and sub-directories in the share.

After a home directory is deleted, if you try to access the same home directory again, a new home directory will automatically be created.

If you have an open file when the home directory is deleted, and you try to save the file, a warning appears:

```
Warning: Make sure the path or filename is correct.
```

```
Save dialog?
```

Click on the `Save` button which saves the file to a new home directory.

### To delete a home directory share

- ◆ To delete the home directory of a specific user, enter the following:

```
CIFS> homedir delete username [domainname]  
Do you want to delete homedir for username (y/n):
```

*username*            The name of the CIFS user. If a CIFS user name includes a space, enter the user name with double quotes.  
  
Respond with *y(es)* or *n(o)* to confirm the deletion.

*domainname*        The domain it is located in.

You can delete all of the home directory shares with the `CIFS> homedir deleteall` command. This also deletes all files and subdirectories in these shares.

After you delete the existing home directories, you can again create the home directories manually or automatically.

### To delete the home directories

- ◆ To delete all home directories, enter the following:

```
CIFS> homedir deleteall  
Do you want to delete all home directories (y/n):
```

Respond with *y(es)* or *n(o)* to confirm the deletion.

After you delete the home directories, you can stop Veritas Access serving home directories by using the `CIFS> set homedirfs` command.

### To disable creation of home directories

- ◆ To specify that there are no home directory file systems, enter the following:

```
CIFS> set homedirfs
```

After these steps, Veritas Access does not serve home directories.

## About CIFS clustering modes

The following clustering modes are supported by Veritas Access:

- Normal
- Clustered Trivial Database (CTDB) - a cluster implementation of the TDB (Trivial database) based on the Berkeley database API

The following operating modes are supported by Veritas Access:

- User
- Domain
- ADS

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 almost all of 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
- Simultaneous access of a share from multiple nodes and therefore better load balancing

## About load balancing for the normal clustering mode

In normal clustering mode, a CIFS share is served from a single node. CIFS users can access an exported share on any Veritas Access node. All of the nodes can concurrently perform file operations. All of the file systems are mounted on every node. The exported shares are also exported from every node.

The following restriction exists for normal clustering mode: only one node at a time can perform file operations on a single share in normal clustering mode. The decision which node is currently allowed to perform the file operations for a specific share is made by the Veritas Access software and is transparent to the CIFS users.

Other issues pertaining to normal clustering mode:

- There is a tie up between a virtual IP address and a share. If a virtual IP address that is serving a share is deleted, then the virtual IP address is needed to reschedule that share on another virtual IP address.
- You can only export the root file system in normal clustering mode.
- A file system cannot be exported as a different share.

When a CIFS share is accessed by a node that is not the owner of that share, Veritas Access transparently redirects the access to the node that is the owner of that share. So, all of the processing for a CIFS share is performed by the node that is designated as the owner of that share.

Use the `CIFS> share show` command to view which virtual IP address is assigned to a share.

Use the `Network> ip addr show` command to view which node is assigned a virtual IP address. This shows which node is the current owner of the exported CIFS shares.

## About load balancing for the ctdb clustering mode

The ctdb-based clustering mode provides a guarantee of data integrity and consistent locking among Veritas Access nodes. A CIFS share can be served from multiple nodes simultaneously and therefore provides better load balancing.

A CIFS share can be served from multiple virtual IP addresses (VIPs) simultaneously. There will not be any tie up between a VIP and a CIFS share. No redistribution of the CIFS share is required while deleting the VIP. A newly-added VIP can be easily used to serve the CIFS share without any administrator intervention.

## About switching the clustering mode

You can switch from normal to ctdb clustering mode or from ctdb to normal clustering mode. You must stop the CIFS server prior to switching to any cluster mode.

See [“About CIFS clustering modes”](#) on page 210.

See [“Switching from normal to ctdb clustering mode”](#) on page 212.

See [“Switching from ctdb to normal clustering mode”](#) on page 215.

### Switching from normal to ctdb clustering mode

You must stop the CIFS server prior to switching to any clustering mode by issuing the `CIFS> server stop` command.

In ctdb clustering mode, if the Veritas Access cluster is joined to the domain, then stopping the CIFS server always results in leaving the join. This is a special case that applies to ctdb clustering mode; this behavior does not occur with normal clustering mode.

**To switch from normal to ctdb clustering mode**

- 1 To check the status of the CIFS server prior to switching from normal to ctdb clustering mode, enter the following:

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

Homedirfs           : fsl
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VTASERVER
Domain User         : administrator
Clustering Mode     : normal
```

- 2 If the CIFS server is running, enter the following:

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

- 3 To set the CIFS clustering mode to ctdb, enter the following:

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

**4** To start the CIFS server, enter the following:

```
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  
VTASSERVER (10.209.110.210) is: 8 seconds
```

```
Time on Domain Controller : Thu Aug 19 15:04:22 2010
```

```
Time on this system : Thu Aug 19 15:04:14 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.
```

**5** To check the status of the CIFS server, enter the following:

```
CIFS> server status
```

```
CIFS Status on ctdb_01 : ONLINE
```

```
CIFS Status on ctdb_02 : ONLINE
```

```
Homedirfs : fs1
```

```
Security : ads
```

```
Domain membership status : Enabled
```

```
Domain : VERITASDOMAIN.COM
```

```
Workgroup : VERITASDOMAIN
```

```
Domain Controller : VTASSERVER
```

```
Domain User : administrator
```

```
Clustering Mode : ctdb
```

## Switching from ctdb to normal clustering mode

You must stop the CIFS server prior to switching to any clustering mode by issuing the `CIFS> server stop` command.

---

**Note:** Domain membership is disabled while stopping the CIFS server in ctdb clustering mode.

---

### To switch from ctdb to normal clustering mode

- 1 To check the status of the CIFS server prior to switching from ctdb to normal clustering mode, enter the following:

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

Homedirfs           : fs1
Security             : ads
Domain membership status : Enabled
Domain               : VERITASDOMAIN.COM
Workgroup            : VERITASDOMAIN
Domain Controller    : VTASSERVER
Domain User          : administrator
Clustering Mode      : ctdb
```

- 2 If the CIFS server is running, enter the following:

```
CIFS> server stop

Disabling membership in AD domain VERITASDOMAIN.COM

Enter password for user `administrator':
Left AD domain VERITASDOMAIN.COM
Stopping CIFS Server .....Success.
```

- 3 To set the CIFS clustering mode to normal, enter the following:

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

**4** To start the CIFS server, enter the following:

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

The skew of the system clock with respect to Domain controller
VTASSERVER (10.209.110.210) is: 8 seconds

Time on Domain Controller : Thu Aug 19 15:47:47 2010
Time on this system : Thu Aug 19 15:47:39 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 a password for user `administrator'
Joined domain VERITASDOMAIN.COM OK
Starting CIFS Server.....Success.
```

**5** To check the status of the CIFS server, enter the following:

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

Homedirfs           : fs1
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VTASSERVER
Domain User         : administrator
Clustering Mode     : normal
```

## About migrating CIFS shares and home directories

You can migrate CIFS shares and home directories from normal to ctdb clustering mode and from ctdb to normal clustering mode.

Veritas Access automatically migrates all CIFS shares and home directories while switching from one clustering mode to another. However, it is not possible to migrate

directory-level shares in the normal clustering mode, because directory-level sharing is not supported in normal clustering mode.

Automatic migration of the content of users (that is, users' home directories) from one file system to another file system while switching home directories is not supported. So, if a Veritas Access administrator changes home directories from fs1 to fs2, then users' home directories are not migrated from fs1 to fs2 automatically.

While migrating from normal to ctdb clustering mode, a simple share is created for each split share, because splitting shares is not supported in ctdb clustering mode.

See [“Migrating CIFS shares and home directories from normal to ctdb clustering mode”](#) on page 218.

See [“Migrating CIFS shares and home directories from ctdb to normal clustering mode”](#) on page 220.

## Migrating CIFS shares and home directories from normal to ctdb clustering mode

### To migrate CIFS shares and home directories from normal to ctdb clustering mode

- 1 To check the CIFS server status to confirm that the current cluster mode is set to normal, enter the following:

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

Homedirfs           : fs1
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VTASERVER
Domain User         : administrator
Clustering Mode     : normal
```

- 2 To list the CIFS shares and home directories, enter the following:

```
CIFS> share show
ShareName FileSystem ShareOptions
share1*   fs1          split,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

CIFS> homedir show
UserName      DomainName
test          Local
administrator VERITASDOMAIN
```

- 3 To stop the CIFS server before changing the clustering mode to ctdb, enter the following:

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

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

- 4 To start the CIFS server in ctdb clustering mode and check the CIFS server status, enter the following:

```
CIFS> server start
```

```
Disabling membership in AD domain VERITASDOMAIN.COM
```

```
Enter a 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  
accessqa_ad.accessqa.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 a password for user `administrator'
```

```
Joined domain VERITASDOMAIN.COM OK
```

```
..Success.
```

```
CIFS> server status
```

```
CIFS Status on ctdb_01 : ONLINE
```

```
CIFS Status on ctdb_02 : ONLINE
```

```
Homedirfs : fs1
```

```
Security : ads
```

```
Domain membership status : Enabled
```

```
Domain : VERITASDOMAIN.COM
```

```
Workgroup : VERITASDOMAIN
```

```
Domain Controller : VTASERVER
```

```
Domain User : administrator
```

```
Clustering Mode : ctdb
```

- 5 To verify that all the CIFS shares and home directories are properly migrated to the ctdb clustering mode, enter the following:

```
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
```

```
CIFS> homedir show
```

```
UserName DomainName
```

```
test Local
```

```
administrator VERITASDOMAIN
```

## Migrating CIFS shares and home directories from ctdb to normal clustering mode

If a file system is exported as multiple CIFS shares in ctdb clustering mode, then while migrating to normal clustering mode, Veritas Access creates only one CIFS share, whichever comes first in the list.

## To migrate a CIFS share and home directory from ctdb to normal clustering mode

- 1 To check the status of the CIFS server, enter the following:

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

Homedirfs           : fs1
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VTASSERVER
Domain User         : administrator
Clustering Mode     : ctdb
```

- 2 To list the CIFS shares and home directories, enter the following:

```
CIFS> share show
ShareName FileSystem      ShareOptions
share1    fs1/access owner=root,group=root,fs_mode=755,rw,noguest
share2    fs1/access owner=root,group=root,fs_mode=755,ro,guest
share3    fs3          owner=root,group=root,fs_mode=1777
share4    fs4          owner=root,group=root,fs_mode=1777,rw

CIFS> homedir show
UserName      DomainName
test          Local
administrator VERITASDOMAIN
```

- 3 To stop the CIFS server to switch the clustering mode to normal, enter the following:

```
CIFS> server stop
```

```
Disabling membership in AD domain VERITASDOMAIN.COM
```

```
Enter password for user `administrator':
```

```
Left AD domain VERITASDOMAIN.COM
```

```
Stopping CIFS Server .....Success.
```

```
CIFS> set clustering_mode normal
```

```
Global option updated. Note: Restart the CIFS server.
```

**4 To start the CIFS server in normal clustering mode, enter the following:**

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

The skew of the system clock with respect to Domain controller
SYMSEVER (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 a 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
Clustering mode
Sharename      FS Name
share1         fs1/Veritas isa
share2         fs1/Veritas isa
Starting CIFS Server.....Success.
```

The warning message indicates that Veritas Access was unable to migrate the directory-level share to normal clustering mode. The rest of the CIFS share and home directory were migrated.

**5 To list the CIFS shares and home directories after migrating to normal clustering mode, enter the following:**

```
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

CIFS> homedir show
UserName   DomainName
test       Local
administrator VERITASDOMAIN
```

## Setting the CIFS aio\_fork option

The `CIFS> set aio_size` option allows you to set an Asynchronous I/O (AIO) read/write size with an unsigned integer.

### To set the aio\_fork option

- ◆ To set the `aio_fork` option, enter the following:

```
CIFS> set aio_size size
```

where *size* is the AIO read/write size.

If *size* is not set to 0, then enable the `aio_fork` option, and set it as an AIO read/write size. If *size* is set to 0, then disable the `aio_fork` option, and set 0 to an AIO read/write size.

For example:

```
CIFS> set aio_size
```

```
set aio_size <size>
```

```
--set aio_fork read/write size.
```

```
size : Unsigned integer or 0 to disable aio
```

```
CIFS> set aio_size 0
```

```
Global option updated. Note: Restart the CIFS server.
```

```
CIFS> set aio_size 1024
```

```
Global option updated. Note: Restart the CIFS server.
```

## About managing local users and groups

When Veritas Access is operating in the standalone mode, only the local users and groups of users can establish CIFS connections and access the home directories and ordinary shares. The Veritas Access local files store the information about these user and group accounts. Local procedures authenticate and authorize these users and groups based on the use of names and passwords. You can manage the local users and groups as described in the rest of this topic.

Accounts for local users can be created, deleted, and information about them can be displayed using the `CIFS> local user` commands.

## Creating a local CIFS user

### To create the new local CIFS user

- ◆ To create a local CIFS user, enter the following:

```
CIFS> local user add username [grouplist]
```

where *username* is the name of the user. The *group*list is a comma-separated list of group names.

For example:

```
CIFS> local user add usr1 grp1,grp2
Adding USER : usr1
Success: User usr1 created successfully
```

### To set the local user password

- ◆ To set the local password, enter the following:

```
CIFS> local password username
```

where *username* is the name of the user whose password you are changing.

For example, to reset the local user password for `usr1`, enter the following:

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

**To display the local CIFS user(s)**

- 1 To display local CIFS users, enter the following:

```
CIFS> local user show [username]
```

where *username* is the name of the user.

For example, to list all local users:

```
CIFS> local user show
List of Users
-----
usr1
usr2
usr3
```

- 2 To display one local user, enter the following:

```
CIFS> local user show usr1
Username      : usr1
UID           : 1000
Groups       : grp1
```

**To delete the local CIFS user**

- ◆ To delete a local CIFS user, enter the following:

```
CIFS> local user delete username
```

where *username* is the name of the local user you want to delete.

For example:

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

### To change a user's group membership

- ◆ To change a user's group membership, enter the following:

```
CIFS> local user members username grouplist
```

where *username* is the local user name being added to the *grouplist*. Group names in the *grouplist* must be separated by commas.

For example:

```
CIFS> local user members usr3 grp1,grp2  
Success: usr3's group modified successfully
```

## About configuring local groups

A local user can be a member of one or more local groups. This group membership is used in the standalone mode to determine if the given user can perform some file operations on an exported share. You can create, delete, and display information about local groups using the `CIFS> local group` command.

## Configuring a local group

### To create a local group

- ◆ To create a local group, enter the following:

```
CIFS> local group add groupname
```

where *groupname* is the name of the local group.

For example:

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

### To list all local groups

- ◆ To list all existing local groups, enter the following:

```
CIFS> local group show [groupname]
```

where *groupname* lists all of the users that belong to that specific group.

For example:

```
CIFS> local group show
List of groups
-----
grp1
grp2
grp3
```

For example:

```
CIFS> local group show grp1
GroupName      UsersList
-----
grp1           usr1, usr2, usr3, usr4
```

### To delete the local CIFS groups

- ◆ To delete the local CIFS group, enter the following:

```
CIFS> local group delete groupname
```

where *groupname* is the name of the local CIFS group.

For example:

```
CIFS> local group delete grp1
Deleting Group: grp1
Success: Group grp1 deleted successfully
```

## Enabling CIFS data migration

Veritas Access provides the following command for enabling CIFS data migration:

```
CIFS> set data_migration yes|no
```

### To enable data migration for the CIFS server

- 1 To enable data migration for the CIFS server, enter the following:

```
CIFS> set data_migration yes
```

- 2 Restart the CIFS server by entering the following command:

```
CIFS> server start
```

- 3 Map the CIFS share on the Windows domain using the *isa\_Cluster\_Name*\root by the Domain Administrator.

- 4 Copy the data with ROBOCOPY by entering the following command in a Windows command prompt:

```
C:\> ROBOCOPY /E /ZB /COPY:DATSO [windows_source_dir] [CIFS_target_dir]
```

Make sure you have the Windows Resource Kit Tools installed.

- 5 Disable the CIFS data migration option after migration completes for CIFS server security by entering the following command:

```
CIFS> set data_migration no
```

- 6 Restart the CIFS server by entering the following command:

```
CIFS> server start
```

# Using Veritas Access with Amazon S3

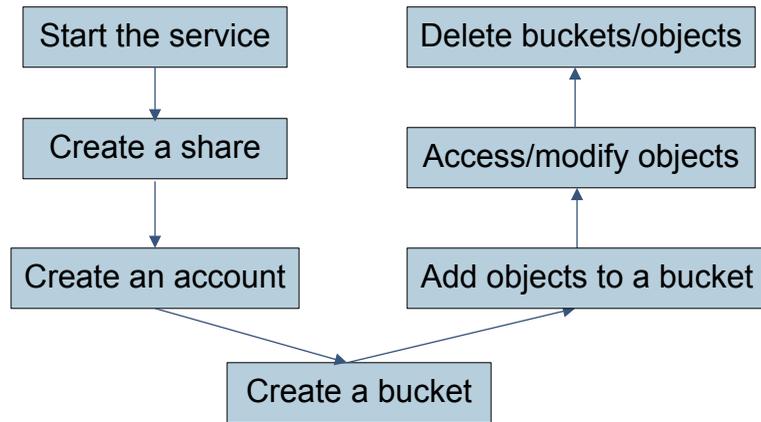
This chapter includes the following topics:

- [About the object access service](#)
- [About the file system hierarchy](#)
- [About access management using S3 Access Control Lists](#)
- [Limitations on using the Amazon S3 protocol](#)
- [Managing the object access service](#)
- [Managing Veritas Access S3 accounts](#)
- [Creating buckets and objects](#)

## About the object access service

The object access service lets you store and retrieve the data that is stored in Veritas Access using the Amazon Simple Storage Service (Amazon S3) protocol. Veritas Access offers unified access, which includes the option to share a file system or a directory in a file system that you can access using both NFS and S3 protocol. You can access data using either of the protocols with a single domain credential.

A bucket maps to a directory inside Veritas File System and an object maps to a file. The object access service in Veritas Access provides a REST interface. Buckets and objects are created, fetched, and deleted using standard HTTP requests.

**Figure 12-1** Workflow of the object access service

See [“Managing the object access service”](#) on page 235.

See [“Managing the Veritas Access S3 share”](#) on page 438.

See [“Managing Veritas Access S3 accounts”](#) on page 236.

See [“Creating buckets and objects”](#) on page 237.

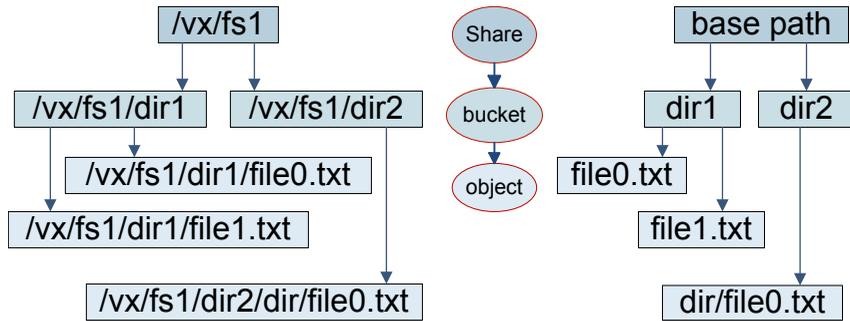
Features of the object access service:

- High availability
- Multipart uploading
- Concurrent access from multiple nodes
- Concurrent access of the same data over NFS and S3
- Canned Access Control Lists

## About the file system hierarchy

In Veritas Access, buckets in S3 are mapped to directories in NFS, and objects in S3 are mapped to files. The object access service requires a base path, for which you can specify any file system or directory. All the buckets and objects are created as relative to the base path.

**Figure 12-2** Example of file system hierarchy mapping



## About access management using S3 Access Control Lists

S3 Access Control Lists (ACLs) let you manage access to buckets and objects.

You can grant basic read or write permissions to other S3 accounts or predefined groups using ACLs. When the object access service receives a request against a resource, it checks the corresponding ACL to verify the access permissions.

- grant** An action that grants permissions by adding the grant elements. Each grant element identifies the grantee and their permission.
- grantee** An S3 account or one of the predefined S3 group for which the access permission is granted.

Veritas Access supports canned ACLs, which are a set of predefined grants. Every canned ACL has a predefined set of grantees and permissions. [Table 12-1](#) lists the set of canned ACLs and the associated predefined grants that Veritas Access supports.

**Table 12-1** Canned ACLs overview

Canned ACL	Applicable to	Permissions added to ACL	Prerequisite
private	bucket and object	Owner gets FULL_CONTROL. No one else has access (default entry).	None

**Table 12-1** Canned ACLs overview (*continued*)

Canned ACL	Applicable to	Permissions added to ACL	Prerequisite
public-read	bucket and object	Owner gets FULL_CONTROL. All S3 users or groups get READ access.	None
public-read-write	bucket and object	Owner gets FULL_CONTROL. All S3 users or groups get READ and WRITE access. Veritas doesn't recommend to granting this permission on a bucket.	None
Authenticated-read	bucket and object	Owner gets FULL_CONTROL. The Authenticated group users get READ access.	A group named "Authenticated". You can use it for any custom grouping purpose.

## Limitations on using the Amazon S3 protocol

The following limitations are related to support for the Amazon S3 protocol.

### List of S3 APIs supported by Veritas Access

The following list describes the S3 APIs that are currently supported by Veritas Access along with any optional parameters:

- Create bucket
- Delete bucket
- Get or list buckets  
Optional parameter: x-amz-acl
- Get bucket info (HEAD)
- Bucket ACLs (GET, PUT)
- Get object  
Optional parameters: if-modified-since, range, if-none-match
- Get object info (HEAD)  
Optional parameters: if-modified-since, range, if-none-match

- Put object
- Delete object
- POST object
- Object ACLs (GET, PUT)
- Multipart uploads (initiate, complete, abort)

## Object and bucket restrictions

[Table 12-2](#) describes the restrictions enforced by the Veritas Access cluster on the S3 client. Configure your S3 clients within these limitations to ensure that Veritas Access works correctly.

**Table 12-2** Object and bucket restrictions

Description	Limit
Maximum recommended concurrent I/O operations	10
Maximum size of a file system or a share	255 TB
Maximum number of objects or files per file system	1 billion
Maximum buckets in a share	10,000
Maximum recommended size of an object that can be PUT using single upload at a time	100 MB
Maximum recommended size of an object that can be uploaded using multipart upload at a time	100 GB

## Multipart uploading restrictions

Veritas Access supports multipart upload in S3. [Table 12-3](#) describes some of the restrictions of the multipart upload function.

**Table 12-3** Multipart uploading restrictions

Item	Limit
Maximum number of parts per upload	10,000
Part size	100 MB The last part can be less than 100 MB.

- Veritas Access does not support the function of listing all the in-progress multipart uploads on a bucket.
- If node failover happens during the multipart uploading process, the uploading fails and you need to upload all the parts again.

## Concurrent access restrictions

This section describes the restrictions of the concurrent access feature.

- When an S3 client tries to read a file which is being written from NFS, it can only receive part of the file that has been written to the NFS server.
- When an NFS v3 client tries to read a file which is being uploaded by an S3 client, the NFS v3 gets a stale file handle after the file is completely uploaded.

## Secure Socket Layer (SSL) limitations

SSL encryption is not supported for the communication between the S3 client and the Veritas Access server. The S3 clients ensure that the REST endpoint of the Veritas Access cluster is addressed as `http://s3.cluster_name:8143`.

# Managing the object access service

This section lists the basics of the object access services. See the `objectaccess` man page for more information.

See [“About the object access service”](#) on page 230.

- Start the service:

```
ObjectAccess> server start
```

---

**Note:** You must have a file system before you start the object access service.

---

You can access the data from any node in the cluster. To balance the load of the high availability function, you need to create a DNS entry for the service.

```
[root@isa ~]# nslookup s3.isacluster
Server:          10.209.194.15
Address:         10.209.194.15#53

Name:   s3.isacluster
Address: 192.168.1.1
Name:   s3.isacluster
```

```
Address: 192.168.1.2
Name:    s3.isacluster
Address: 192.168.1.3
Name:    s3.isacluster
Address: 192.168.1.4
Name:    s3.isacluster
Address: 192.168.1.5
```

If you set the virtual IPs in DNS, the S3 client can simultaneously connect to either of the nodes. In the above example, `s3` needs to be prefixed to the cluster name in the DNS entries like `s3.cluster_name`.

- Check the status of the service:

```
ObjectAccess> server status
```

```
ObjectAccess Status on CLUSTERNAME_01 : ONLINE
ObjectAccess Status on CLUSTERNAME_02 : ONLINE
```

- Stop the service:

```
ObjectAccess> server stop
```

- Check all the configurable options of the service:

```
ObjectAccess> show
```

```
Name          Value
=====
ssl_enabled   no
port          8143
server        http://cluster_name:8143
```

## Managing Veritas Access S3 accounts

You need an S3 account to manage the S3 shares.

- You need to have an S3 share before you create the account to it.
- You can only create an S3 account for the file systems that are available for S3.
- Veritas Access only supports users from LDAP and NIS. You must have configured LDAP and NIS before you add users in the S3 account database. See [“About configuring LDAP settings”](#) on page 74.

See “Creating a file system” on page 346.

### 1 Create an account:

```
ObjectAccess> account add username export_dir
```

```
ObjectAccess> account add ftpuser /vx/ForS3
```

Account	Share	AccessKey	SecretKey
/vx/ForS3:ftpuser	/vx/ForS3	OGQxZDI5MjdmNWRiZjhi	ZWE1MTQzN2ExOWVhODg4YzAxNWEzYzZcwMTFlMzg3

When you create the account, access key and secret key are also created, which are used to access the object access server.

### 2 You can check the information of all the available accounts:

```
ObjectAccess> account show
```

Account	Share	AccessKey	SecretKey
/vx/Mp:manila	/vx/Mp	MzM0ZjllMGE3YWJiNmFi	MWY1OGQzMTVlNzUzZmZmNGE2Njg0N2E3ZjY3YWVm
/vx/Mp:ftpuser	/vx/Mp	NDhkMTM3Njg1MjQyMmE1	YTNhMzQzMzNmNjIzZWExMjZjYmZlYWI5ZDQxMmQy
/vx/ForS3:manila	/vx/ForS3	N2I3Mjc1NjhkZTliY2Mx	Mzg2NTAyNmFjYTQ4MjlkNWU1ZDgzMjdkMDk1ZWQy
/vx/Mp:root	/vx/Mp	NmRmNDVmMmFhMDVjMGMw	MzZjZTBiMjBlZjIyZTM0MmJlYjJhNzU3ZmRlNjRh
/vx/FS_RC2:support	/vx/FS_RC2	MjQ4MTI1YmFiNTEyZTEz	Mjg0OTczZmRiYmE0ODM3ZjdhYmIyODY5ZWE1MTYy

### 3 You can delete an S3 account:

```
ObjectAccess> account delete username export_dir
```

```
ObjectAccess> account delete ftpuser /vx/ForS3
```

```
ACCESS ObjectAccess SUCCESS V-288-0 account '/vx/ForS3:ftpuser'\
has been deleted successfully
```

See the `objectaccess` man page for more information.

## Creating buckets and objects

When you create buckets or objects within an S3 share, Veritas Access maps them to directories or files to the NFS share. Then you can access the buckets or objects from NFS. By default, both buckets and objects are private.

## Creating a bucket

Creating a bucket also creates a directory inside a share. Although S3 supports an unlimited number of buckets, the number must be within the limits for the directories in the file system. A bucket name should be unique across a file system or a share.

The following are the allowed characters for naming buckets:

```
(^[a-zA-z0-9_]{1,255}$)
```

In Veritas Access, if you create a directory from NFS that does not follow the bucket naming convention, the directory is not visible from S3.

You can access a bucket using path-style URLs:

```
hostname:      s3.cluster name.com
bucketname:    bucket
URL:           http://s3.cluster name.com/bucket
```

## Creating an object

The relative path of the file from the base path of the share is known as the object key. An object has a key, data, and metadata. The object key uniquely identifies the object in a bucket.

When you create an object, you create a file inside a share. If the path of the object does not exist, a corresponding directory is created along with the object.

Consequently you cannot use any prefix of the path to create an object due to repeated paths or conflicting paths.

For example, if you create `veritas/access/1.txt`, you cannot create `veritas` or `veritas/access` as they already exist. You cannot create `veritas/access/1.txt/d1/file.txt`, as you can create only an object under a directory instead of an object.

# Configuring your FTP server

This chapter includes the following topics:

- [About FTP](#)
- [Creating the FTP home directory](#)
- [Using the FTP server commands](#)
- [About FTP server options](#)
- [Customizing the FTP server options](#)
- [Administering the FTP sessions](#)
- [Uploading the FTP logs](#)
- [Administering the FTP local user accounts](#)
- [About the settings for the FTP local user accounts](#)
- [Configuring settings for the FTP local user accounts](#)

## About FTP

The file transfer protocol (FTP) server feature allows clients to access files on the Veritas Access servers using the FTP protocol. The FTP service provides secure/non-secure access by FTP to files in the Veritas Access servers. The FTP service runs on all of the nodes in the cluster and provides simultaneous read and write access to the files. The FTP service also provides configurable anonymous access to the filer.

By default, the FTP server is not running. You can start the FTP server using the `FTP> server start` command. The FTP server starts on the standard FTP port 21.

The Veritas Access FTP service does not support transparent failover. During failover due to either a shutdown or a restart of the server, the FTP client loses its connection to the server. As a consequence, any upload or download to the FTP service during the failover fails. Restart any upload or download to the FTP service from the beginning after the connection to the FTP service has been re-established.

## Creating the FTP home directory

Veritas Access can act as an FTP server for LDAP, NIS, or AD users, or local users.

When a user logs into the FTP server for the first time, Veritas Access retrieves the user's home directory information from the authentication server. The authentication server can be an LDAP, NIS, or AD server.

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 the `create_homedirs` option is set to `yes`:

- For NIS users: Create the directory *nisusername* in the `homedir_path`. For example: `/vx/fs1/ftphomes/nisuser1`.
- For LDAP users: Create the directory *ldapusername* in the `homedir_path`. For example: `/vx/fs1/ftphomes/ldapuser1`.
- For AD users: The full string *domainname\username* identifies the Veritas Access user. Create the directory *domainname\username* in the `homedir_path`. For example: `/vx/fs1/ftphomes/mydomain\aduser1`.
- For local users: The home directory is specified as *localusername*. Veritas Access creates the directory *localusername* in the `homedir_path`. For example: `/vx/fs1/ftphomes/localuser1`.

# Using the FTP server commands

The `FTP> server` commands start, stop, and display the status of the FTP server.

## To display the FTP server status

- ◆ To display the FTP server status, enter

```
FTP> server status

FTP Status on access_01 : OFFLINE
FTP Status on access_02 : OFFLINE
```

## To start the FTP server

- 1 If the attribute `user_logon` is set to `yes` (the default value), set a value for `homedir_path`.

The `homedir_path` must be set before the FTP server can start.

```
FTP> set homedir_path pathname
```

Where:

*pathname* Specifies the location of the login directory for users. Valid values include any path that starts with `/vx/`.

- 2 To start the FTP server, enter the following:

```
FTP> server start
```

To check server status, enter the following:

```
FTP> server status

FTP Status on access_01 : ONLINE
FTP Status on access_02 : ONLINE
```

**To stop the FTP server**

- ◆ To stop the FTP server, enter the following:

```
FTP> server stop
```

To check the server status, enter the following:

```
FTP> server status
```

```
FTP Status on access_01 : OFFLINE
```

```
FTP Status on access_02 : OFFLINE
```

## About FTP server options

Veritas Access lets you set various configurable options for the FTP server.

For the changes to take effect, restart the FTP server.

**Table 13-1** FTP options

Option	Definition
<code>allow_delete</code>	Specifies whether or not to allow users to delete files on the FTP server. This option only applies to users. It does not apply to anonymous logins. Anonymous logins are never allowed to delete files.  Enter <i>yes</i> (default) to allow users to delete files on the FTP server. Enter <i>no</i> to prevent users from deleting files on the FTP server.
<code>allow_non_ssl</code>	Specifies whether or not to allow non-secure (plain-text) logins into the FTP server. Enter <i>yes</i> (default) to allow non-secure (plain-text) logins to succeed. Enter <i>no</i> to allow non-secure (plain-text) logins to fail.
<code>anonymous_login_dir</code>	Specifies the login directory for anonymous users. Valid values of this parameter start with <i>/vx/</i> . Make sure that the anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to read files in <i>login_directory</i> .
<code>anonymous_logon</code>	Tells the FTP server whether or not to allow anonymous logons. Enter <i>yes</i> to allow anonymous users to log on to the FTP server. Enter <i>no</i> (default) to not allow anonymous logons.

**Table 13-1** FTP options (*continued*)

Option	Definition
<code>anonymous_write</code>	Specifies whether or not anonymous users have the [write] value in their <i>login_directory</i> . Enter <i>yes</i> to allow anonymous users to modify contents of their <i>login_directory</i> . Enter <i>no</i> (default) to not allow anonymous users to modify the contents of their <i>login_directory</i> . Make sure that the anonymous user (UID:40 GID:49 UNAME:ftp) has the appropriate permissions to modify files in their <i>login_directory</i> .
<code>chroot_users</code>	Specifies whether users should be restricted to their home directories. A value of <i>yes</i> limits users to their home directory. A value of <i>no</i> allows users to view files in parent directories. Users are restricted by their <i>homedir_path</i> . If security is local, then <code>chroot_users</code> should be set to <i>yes</i> .
<code>create_homedirs</code>	Specifies if home directories should be created when a user logs in, if the home directory does not exist. A value of <i>yes</i> allows FTP to create a user's home directory, if it does not already exist. If the value is <i>no</i> , then a home directory should exist for this user, and the user should have permissions to read and execute in this directory. Otherwise, the login fails.
<code>homedir_path</code>	Specifies the location of the login directory for users. Valid values include any path that starts with <code>/vx/</code> . This option is required if <code>user_logon</code> is set to <i>yes</i> .
<code>idle_timeout</code>	Specifies the amount of time in minutes after which an idle connection is disconnected. Valid values for <i>time_in_minutes</i> range from 1 to 600 (default value is 15 minutes).
<code>listen_ipv6</code>	Specifies whether the FTP service should listen on IPv6 for connections. Valid values for this parameter are <i>yes</i> or <i>no</i> . The default value is <i>no</i> .
<code>listen_port</code>	Specifies the port number on which the FTP service listens for connections. Valid values for this parameter range from 10-1023. The default value is 21.
<code>max_connections</code>	Specifies the maximum number of simultaneous FTP clients allowed. Valid values for this parameter range from 1-9999. The default value is 2000.
<code>max_conn_per_client</code>	Specifies the maximum number of simultaneous FTP connections that are allowed from a single client IP address. Valid values for this parameter range from 1-9999. The default value is 2000.

**Table 13-1** FTP options (*continued*)

Option	Definition
<code>passive_port_range</code>	<p>Specifies the range of port numbers to listen on for passive FTP transfers. The <i>port_range</i> defines a range that is specified as startingport:endingport. A <i>port_range</i> 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.</p>
<code>security</code>	<p>Specifies the type of users that are allowed to log in to the FTP server. Enter <i>nis_ldap</i> (default) to allow users with accounts configured on NIS or LDAP servers to log in to the FTP server. Users that are created with the <code>FTP &gt; local user add</code> command cannot log in.</p> <p>Enter <i>local</i> to allow users with accounts created with the <code>FTP&gt; local user add</code> command to log in to the FTP server. NIS and LDAP users cannot log in.</p> <p>The <i>ads</i> option allows access to users configured on Windows Active Directory as specified in the <code>CIFS&gt; show</code> command. NIS, LDAP, and local users are not allowed to log in.</p>
<code>umask</code>	<p>Specifies the mask for permissions with which files or directories are created using FTP.</p> <p>If the <i>file_umask</i> is set to 177, then new files and directories are created with permissions 600, which defines <code>rw-----</code>. The owner of the file or directory has read and write permissions to the file or directory. Members in the users group do not have read or write permissions.</p>
<code>user_logon</code>	<p>Specifies whether to allow FTP access for users. A value of <i>yes</i> allows normal users (non-anonymous users) to log in.</p> <p>If <i>user_logon</i> is set to <i>yes</i>, then the <i>homedir_path</i> also must be set or the FTP server cannot start.</p>

## Customizing the FTP server options

The `FTP> set` commands let you set various configurable options for the FTP server.

See [“About FTP server options”](#) on page 242.

For the changes to take effect, the FTP server must be restarted.

## To change the FTP server options

- 1 To view the current settings, enter the following:

```
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
```

- 2 To change the required server options, use the set command.

For example, to enable anonymous logons, enter the following:

```
FTP> set anonymous_logon yes
```

Changes would be applicable after restart of FTP service.  
 Success.

**3** To view the pending command changes, enter the following:

```
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         no                 yes
anonymous_write         no
anonymous_login_dir     /vx/ftpanon
allow_anon_fxp          no
user_logon              yes
homedir_path            /vx/ftphomes
allow_delete            yes
security                local
allow_user_fxp          no
chroot_users            yes
create_homedirs         yes
```

- 4** To implement the changes, you must stop and restart the FTP server.

Enter the following:

```
FTP> server stop
FTP> server start
```

- 5** To view the new settings, enter the following:

```
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
```

## Administering the FTP sessions

### To display the current FTP sessions

- ◆ To display the current FTP sessions, enter the following:

```
FTP> session show
Max Sessions : 2000

Nodename  Current Sessions
-----
access_01      4
access_02      2
```

### To display the FTP session details

- ◆ To display the details in the FTP sessions, enter the following:

```
FTP> session showdetail [filter_options]
```

where *filter\_options* display the details of the sessions under specific headings. Filter options can be combined by using ','. If multiple filter options are used, sessions matching all of the filter options are displayed.

For example, to display all of the session details, enter the following:

```
FTP> session showdetail
Session ID      User      Client IP      Server IP      State  File
-----
access_01.1111 user1     10.209.105.219 10.209.105.111 IDLE
access_01.1112 user2     10.209.106.11  10.209.105.111 IDLE
access_02.1113 user3     10.209.107.21  10.209.105.112 IDLE
access_01.1117 user4     10.209.105.219 10.209.105.111 DL      file123
access_02.1118 user1     10.209.105.219 10.209.105.111 UL      file345
access_01.1121 user5     10.209.111.219 10.209.105.112 IDLE
```

For example, to display the details of the current FTP sessions to the Server IP (10.209.105.112), originating from the Client IP (10.209.107.21), enter the following:

```
FTP> session showdetail server_ip=10.209.105.112,
client_ip=10.209.107.21
Session ID      User      Client IP      Server IP      State  File
-----
access_02.1113 user3     10.209.107.21  10.209.105.112 IDLE
```

### To terminate an FTP session

- ◆ To terminate one of the FTP sessions that are displayed in the `FTP> session showdetail` command, enter the following:

```
FTP> session terminate session_id
```

where *session\_id* is the unique identifier for each FTP session that is displayed in the `FTP> session showdetail` output.

```
FTP> session terminate access_02.1113
Session access_02.1113 terminated
```

## Uploading the FTP logs

The `FTP> logupload` command lets you upload the FTP server logs to a specified URL.

### To upload the FTP server logs

- ◆ To upload the FTP server logs to a specified URL, enter the following:

```
FTP> logupload url [nodename]
```

<code>url</code>	The URL where the FTP logs are uploaded. The URL supports both FTP and SCP (secure copy protocol). If a node name is specified, only the logs from that node are uploaded.  The default name for the uploaded file is <code>ftp_log.tar.gz</code> .  Passwords that are added directly to the URL are not supported.
<code>nodename</code>	The node on which the operation occurs. Enter the value <code>all</code> for the operation to occur on all of the nodes in the cluster.
<code>password</code>	Use the password you already set up on the node to which you upload the logs.

For example, to upload the logs from all of the nodes to an SCP-based URL:

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

For example, to upload the logs from `access_1` to an FTP-based URL:

```
FTP> logupload ftp://user@host:/path/to/directory access_1
Password:
Collecting FTP logs, please wait....
Uploading the logs to ftp://root@host:/path/to/directory,
please wait...done
```

## Administering the FTP local user accounts

The `FTP> local user` commands let you create and manage local user accounts on the FTP server.

When you add a local user account, the user's home directory is created automatically on the FTP server. User home directories on the FTP server are specified by *path/username* where *path* is the home directory path configured by the `FTP > set homedir_path` command.

All users are limited to their home directories and are not allowed to access files on the FTP server beyond their home directories.

### To add a local user account

- 1 To add a local user account, enter the following:

```
FTP> local user add username
```

where *username* is the name of the user whose account you want to add.

- 2 When the password prompt appears, enter a password for the local user.
- 3 Type the password again for verification.

For example:

```
FTP > local user add user1
Input password for user1.
Enter password:
Re-enter password:
Success.
```

### To change a password for a local user

- 1 To change a password for a local user, enter the following:

```
FTP> local user passwd username
```

where *username* is the name of the user whose password you want to change.

- 2 When the password prompt appears, enter a new password, then type the password again for verification.

For example:

```
FTP > local user passwd user1
Enter password:
Re-enter password:
Success.
```

**To delete a local user account**

- ◆ To delete a local user account, enter the following:

```
FTP> local user delete username
```

where *username* is the name of the user whose account you want to delete.

For example:

```
FTP > local user delete user1  
Success.
```

When you delete a local user account, the local user's home directory is not deleted.

**To show local user accounts**

- ◆ To show local user accounts (and account settings) configured on the FTP server, enter the following:

```
FTP> local user show
```

USER	HOMEDIR	BANDWIDTH	MAX_CONN
localftp1	/localftp1	-	1000
localftp2	/localftp2	20 MB/s	-
localftp3	/test/asfta	10 MB/s	-
localftp4	/localftp4	-	20
test	/test	103 MB/s	10003
test2	/test2	-	-

## About the settings for the FTP local user accounts

By default, local user accounts on the FTP server have no limits for the following:

- Bandwidth.
- Number of simultaneous connections.

To configure limits for these options, use the `FTP> user local set` commands.

You can also use the `FTP> local user set` command to specify home directories for local users accounts.

Local user changes are effective immediately for new connections. You do not need to restart the FTP server.

See [“Configuring settings for the FTP local user accounts”](#) on page 253.

**Table 13-2** FTP local user options

Option	Definition
bandwidth	Specifies the maximum bandwidth (in MB/second) for a local user account on the FTP server. By default, there is no limit on the bandwidth for local users.
max_connections	Specifies the maximum number of simultaneous connections a local user can have to each node in the cluster. By default there is no limit to the number of connections a local user can have to the FTP server.
homedir	<p>Specifies the home directory for a local user account.</p> <p>The home directory you configure for a local user account is created relative to the home directory path that is configured by the <code>FTP &gt; set homedir_path</code> command.</p> <p>The default home directory value for local user accounts is <i>username</i> where <i>username</i> is the login name for the local user account.</p> <p>For example, if the home directory path is set to <code>/vx/fsl/ftp_home</code> and the user name is <code>user1</code>, the default home directory for <code>user1</code> is <code>/vx/fsl/ftp_home/user1</code></p> <p>Changes to this value are applicable for any new connections. Configuring a new home directory location does not migrate any existing data in a local user's current home directory to the new home directory.</p>

# Configuring settings for the FTP local user accounts

## To show local user settings

- ◆ To show the current settings for local user accounts, enter the following:

```
FTP> local user show
```

USER	HOMEDIR	BANDWIDTH	MAX_CONN
----	-----	-----	-----
localftp1	/localftp1	-	1000
localftp2	/localftp2	20 MB/s	-
localftp3	/test/asfta	10 MB/s	-
localftp4	/localftp4	-	20
test	/test	103 MB/s	10003
test2	/test2	-	-

## To set bandwidth

- ◆ To set the maximum bandwidth for a local user account, enter the following:

```
FTP> local user set bandwidth username max_value
```

**username**                Specifies the name of a user account.

**max\_value**              Specifies the maximum upload bandwidth value (measured in MB/second) for the user's account.

For example:

```
FTP > local user set bandwidth user2 40000
Success.
```

### To set maximum connections

- ◆ To set the maximum number of simultaneous connections a local user can have to the FTP server, enter the following:

```
FTP> local user set max_connections username  
number
```

*username* Specifies the name of a user account.

*number* Specifies the maximum number of simultaneous connects a user can have to the FTP server.

For example:

```
FTP> local user set max_connections user2 1000  
Success.
```

### To set the home directory

- ◆ To set the home directory for a local user account, enter the following:

```
FTP> local user set homedir username  
dir_name
```

*username* Specifies that name of a user account.

*dir\_name* Specifies the name of the home directory for the local user account.

For example:

```
FTP> local user set homedir user2 home  
Success.
```

The home directory you configure for a local user account is relative to the home directory path that is configured by the `FTP> set homedir_path` command.

Changes to this value are applicable for any new connections. Configuring a new home directory location does not migrate any existing data in a local user's current home directory to the new home directory.

# Configuring Veritas Access with OpenStack Cinder

This chapter includes the following topics:

- [About the Veritas Access integration with OpenStack Cinder](#)
- [About the Veritas Access integration with OpenStack Cinder architecture](#)
- [Configuring Veritas Access with OpenStack Cinder](#)
- [Configuring OpenStack Cinder](#)

## About the Veritas Access integration with OpenStack Cinder

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources in a data center. OpenStack provides a dashboard that lets you provision resources using a web interface.

Cinder is a block storage service for OpenStack. Cinder provides the infrastructure for managing volumes in OpenStack. Cinder volumes provide persistent storage to guest virtual machines (known as instances) that manage OpenStack compute software.

Veritas Access is integrated with OpenStack Cinder, which provides the ability for OpenStack instances to use the storage hosted by Veritas Access.

**Table 14-1** Mapping of OpenStack Cinder operations to Veritas Access

Operation in OpenStack Cinder	Operation in Veritas Access
Create and delete volumes	Create and delete files.
Attach and detach the volumes to virtual machines	This operation occurs on the OpenStack controller node.  This operation is not applicable in Veritas Access.
Create and delete snapshots of the volumes	Create and delete file system snapshots.
Create a volume from a snapshot	This operation occurs on the OpenStack controller node.  This operation is not applicable in Veritas Access.
Copy images to volumes	This operation occurs on the OpenStack controller node.  This operation is not applicable in Veritas Access.
Copy volumes to images	This operation occurs on the OpenStack controller node.  This operation is not applicable in Veritas Access.
Extend volumes	Extending files.

---

**Note:** To perform these operations, you need to use the OpenStack Cinder commands, not the Veritas Access commands.

---

The Veritas NFS OpenStack Cinder driver is a Python script that is checked in to the OpenStack source code in the public domain. To use the Veritas Access integration with OpenStack Cinder, you need to make some configuration changes on the OpenStack controller node.

For the supported OpenStack versions for running the OpenStack Cinder driver, see the *Veritas Access Installation Guide*.

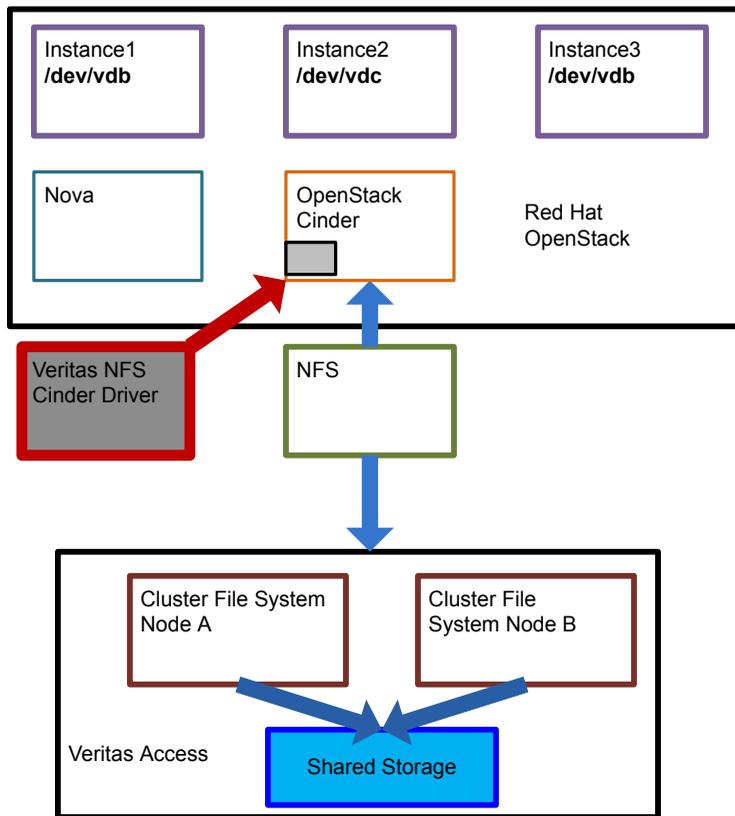
See [“Configuring OpenStack Cinder”](#) on page 261.

# About the Veritas Access integration with OpenStack Cinder architecture

Figure 14-1 describes the Veritas Access integration with OpenStack Cinder architecture.

OpenStack instances are the individual virtual machines running on physical compute nodes. The compute service, Nova, manages the OpenStack instances.

Figure 14-1 Veritas Access integration with OpenStack Cinder architecture



# Configuring Veritas Access with OpenStack Cinder

## To show all your NFS shares

- ◆ To show all your NFS shares that are exported from Veritas Access, enter the following:

```
OPENSTACK> cinder share show
```

For example:

```
OPENSTACK> cinder share show  
/vx/fs1 *(rw,no_root_squash)
```

```
OPENSTACK> cinder share show  
/vx/o_fs 2001:21::/120 (rw,sync,no_root_squash)
```

## To share and export a file system

- ◆ To share and export a file system, enter the following:

```
OPENSTACK> cinder share add export-dir world|client
```

After issuing this command, OpenStack Cinder will be able to mount the exported file system using NFS.

*export-dir* Specifies the path of the directory that needs to be exported to the client.

The directory path should start with /vx and only the following characters are allowed:

```
'a-zAZ0-9_/@+.=:.'
```

*world* Specifies if the NFS export directory is intended for everyone.

*client*

Exports the directory with the specified options.

Clients may be specified in the following ways:

- **Single host**  
Specify a host either by an abbreviated name recognized by the resolver, the fully qualified domain name, or an IP address.
- **Netgroups**  
Netgroups may be given as @group. Only the host part of each netgroup member is considered when checking for membership.
- **IP networks**  
You can 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.

To re-export new options to an existing share, the new options will be updated after the command is run.

For example:

```
OPENSTACK> cinder share add /vx/fs1 world
Exporting /vs/fs1 with options rw,no_root_squash

OPENSTACK> cinder share add /vx/o_fs 2001:21::/120
Exporting /vx/o_fs with options rw,sync,no_root_squash Success.
```

### To delete the exported file system

- ◆ To delete (or unshare) the exported file system, enter the following:

```
OPENSTACK> cinder share delete export-dir client
```

For example:

```
OPENSTACK> cinder share delete /vx/fs1 world
Removing export path */vx/fs1
Success.
```

## To start or display the status of the OpenStack Cinder service

- 1 To start the OpenStack Cinder service, enter the following:

```
OPENSTACK> cinder service start
```

The `OPENSTACK> cinder service start` command needs the NFS service to be up for exporting any mount point using NFS. The `OPENSTACK> cinder service start` command internally starts the NFS service by running the command `NFS> server start` if the NFS service has not been started. There is no `OPENSTACK> cinder service stop` command. If you need to stop NFS mounts from being exported, use the `NFS> server stop` command.

For example:

```
OPENSTACK> cinder server start  
..Success.
```

- 2 To display the status of the OpenStack Cinder service, enter the following:

```
OPENSTACK> cinder service status
```

For example:

```
OPENSTACK> cinder server status  
NFS Status on access_01 : ONLINE  
NFS Status on access_02 : ONLINE
```

## To display configuration changes that need to be done on the OpenStack controller node

- ◆ To display all the configuration changes that need to be done on the OpenStack controller node, enter the following:

```
OPENSTACK> cinder configure export-dir
```

*export-dir*

Specifies the path of the directory that needs to be exported to the client.

The directory path should start with `/vx` and only the following characters are allowed:

```
'a-zAZ0-9_/@+.=:.'
```

For example:

```
OPENSTACK> cinder configure /vx/fs1
```

# Configuring OpenStack Cinder

To create a new volume backend named **ACCESS\_HDD** in OpenStack Cinder

- 1 Add the following configuration block in the `/etc/cinder/cinder.conf` file on your OpenStack controller node.

```
enabled_backends=access-1
[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
```

Add the lines from the configuration block at the bottom of the file.

<code>volume_driver</code>	Name of the Veritas Access Cinder driver.
<code>volume_backend_name</code>	For this example, <code>ACCESS_HDD</code> is used. This name can be different for each NFS share. If several backends have the same name, the OpenStack Cinder scheduler decides in which backend to create the volume.
<code>nfs_shares_config</code>	This file has the share details in the form of <code>vip:/exported_dir</code> .
<code>nfs_mount_point_base</code>	Mount point where the share will be mounted on OpenStack Cinder. If the directory does not exist, create it. Make sure that the <code>Cinder</code> user has write permission on this directory.
<code>nfs_sparsed_volumes</code>	Preallocate or sparse files.
<code>nfs_disk_util</code>	Free space calculation.
<code>nfs_mount_options</code>	These are the mount options OpenStack Cinder uses to NFS mount.

This same configuration information for adding to the `/etc/cinder/cinder.conf` file can be obtained by running the `OPENSTACK CINDER> configure export_dir` command.

- 2 Append the following in the `/etc/cinder/access_share_hdd` file on your OpenStack controller node:

```
vip:/vx/fs1
```

Use one of the virtual IPs for `vip`:

- 192.1.1.190
- 192.1.1.191
- 192.1.1.192
- 192.1.1.193
- 192.1.1.199

You can obtain Veritas Access virtual IPs using the `OPENSTACK> cinder configure export-dir` option.

- 3 Create the `/etc/cinder/access_share_hdd` file at the root prompt, and update it with the NFS share details.

```
# cnfs_sata_hdd(keystone_admin)]# cat /etc/cinder/access_share_hdd  
192.1.1.190:/vx/fs1
```

- 4 The Veritas Access package includes the Veritas Access OpenStack Cinder driver, which is a Python script. The OpenStack Cinder driver is located at `/opt/SYMCnas/scripts/OpenStack/veritas_cnfs.py` on the Veritas Access node. Copy the `veritas_cnfs.py` file to `/usr/lib/python2.6/site-packages/cinder/volume/drivers/veritas_cnfs.py` if you are using the Python 2.6 release.

If you are using the OpenStack Kilo version of RDO, the file is located at:

```
/usr/lib/python2.7/site-packages/cinder/volume/drivers/veritas_cnfs.py
```

- 5 Make sure that the NFS mount point on the OpenStack controller node has the right permission for the cinder user. The cinder user should have write permission on the NFS mount point. Set the permission using the following command.

```
# setfacl -m u:cinder:rwX /cinder/cnfs/cnfs_sata_hdd
```

**6 Restart the OpenStack Cinder driver.**

```
# cnfs_sata_hdd(keystone_admin)]# /etc/init.d/openstack-cinder-volume
restart
Stopping openstack-cinder-volume: [ OK ]
Starting openstack-cinder-volume: [ OK ]
```

Restarting the OpenStack Cinder driver picks up the latest configuration file changes.

After restarting the OpenStack Cinder driver, `/vx/fs1` is NFS-mounted as per the instructions provided in the `/etc/cinder/access_share_hdd` file.

```
# cnfs_sata_hdd(keystone_admin)]# mount |grep /vx/fs1
192.1.1.190:/vx/fs1 on
cnfs_sata_hdd/e6c0baa5fb02d5c6f05f964423fecalf type nfs
(rw,nfsvers=3,addr=10.182.98.20)
```

You can obtain OpenStack Cinder log files by navigating to:

```
/var/log/cinder/volume.log
```

**7 If you are using OpenStack RDO, use these steps to restart the OpenStack Cinder driver.**

Login to the OpenStack controller node.

For example:

```
source /root/keystonerc_admin
```

Restart the services using the following command:

```
(keystone_admin)]# openstack-service restart openstack-cinder-volume
```

For more information, refer to the *OpenStack Administration Guide*.

**8 On the OpenStack controller node, create a volume type named `isa_vol_type`.**

This volume type is used to link to the volume backend.

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]#
cinder type-create isa_vol_type
+-----+-----+
| ID | Name |
+-----+-----+
| d854a6ad-63bd-42fa-8458-a1a4fadd04b7 | isa_vol_type |
+-----+-----+
```

**9 Link the volume type with the ACCESS\_HDD back end.**

```
[root@cl059-r720xd-111046cnfs_sata_hdd(keystone_admin)]# cinder type-key
isa_vol_type set volume_backend_name=ACCESS_HDD
```

**10 Create a volume of size 1gb.**

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder create --volume-type
isa_vol_type --display-name isa_voll 1
```

Property	Value
attachments	[]
availability_zone	nova
bootable	false
created_at	2014-02-08T01:47:25.726803
display_description	None
display_name	isa_voll
id	disk ID 1
metadata	{}
size	1
snapshot_id	None
source_volid	None
status	creating
volume_type	isa_vol_type

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder list
```

ID	Status	Display Name	Size	Volume Type	Bootable	Attached to
disk ID 1	available	isa_voll	1	isa_vol_type	false	

**11 Extend the volume to 2gb.**

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder extend isa_voll 2
```

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder list
```

ID	Status	Display Name	Size	Volume Type	Bootable	Attached to
disk ID 1	available	isa_voll	2	isa_vol_type	false	

## 12 Create a snapshot.

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder snapshot-create
--display-name isa_voll-snap isa_voll
```

```
+-----+-----+
| Property | Value |
+-----+-----+
| created_at | 2014-02-08T01:51:17.362501 |
| display_description | None |
| display_name | isa_voll-snap |
| id | disk ID 1 |
| metadata | {} |
| size | 2 |
| status | creating |
| volume_id | 52145a91-77e5-4a68-b5e0-df66353c0591 |
```

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder snapshot-list
```

```
+-----+-----+-----+-----+-----+
| ID | Volume ID | Status | Display Name | Size |
+-----+-----+-----+-----+-----+
| disk ID 1 | 52145a91-77e5-4a68-b5e0-df66353c0591 | available | isa_voll-snap | 2 |
+-----+-----+-----+-----+-----+
```

## 13 Create a volume from a snapshot.

```
[root@cl059-r720xd-111046 cnfs_sata_hdd(keystone_admin)]# cinder
create --snapshot-id e9dda50f-1075-407a-9cb1-3ab0697d274a --display-name
isa-vol2 2
```

```
+-----+-----+
| Property | Value |
+-----+-----+
| attachments | [] |
| availability_zone | nova |
| bootable | false |
| created_at | 2014-02-08T01:57:11.558339 |
```

# Configuring Veritas Access with OpenStack Manila

This chapter includes the following topics:

- [About the Veritas Access integration with OpenStack Manila](#)
- [OpenStack Manila use cases](#)
- [Configuring Veritas Access to work with OpenStack Manila](#)

## About the Veritas Access integration with OpenStack Manila

OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources in a data center. OpenStack provides a dashboard that lets you provision resources using a web interface.

OpenStack Cinder had the limitation of not being able to share a block device simultaneously between virtual machines. OpenStack Manila solves this problem. OpenStack Manila provides a shared file system as a service. Using OpenStack Manila, you can share a single file system between multiple virtual machines.

Veritas Access is integrated with OpenStack Manila through a OpenStack Manila driver that lets you share Veritas Access file systems with virtual machines on OpenStack.

For the supported OpenStack versions for running the OpenStack Manila driver, see the *Veritas Access Installation Guide*.

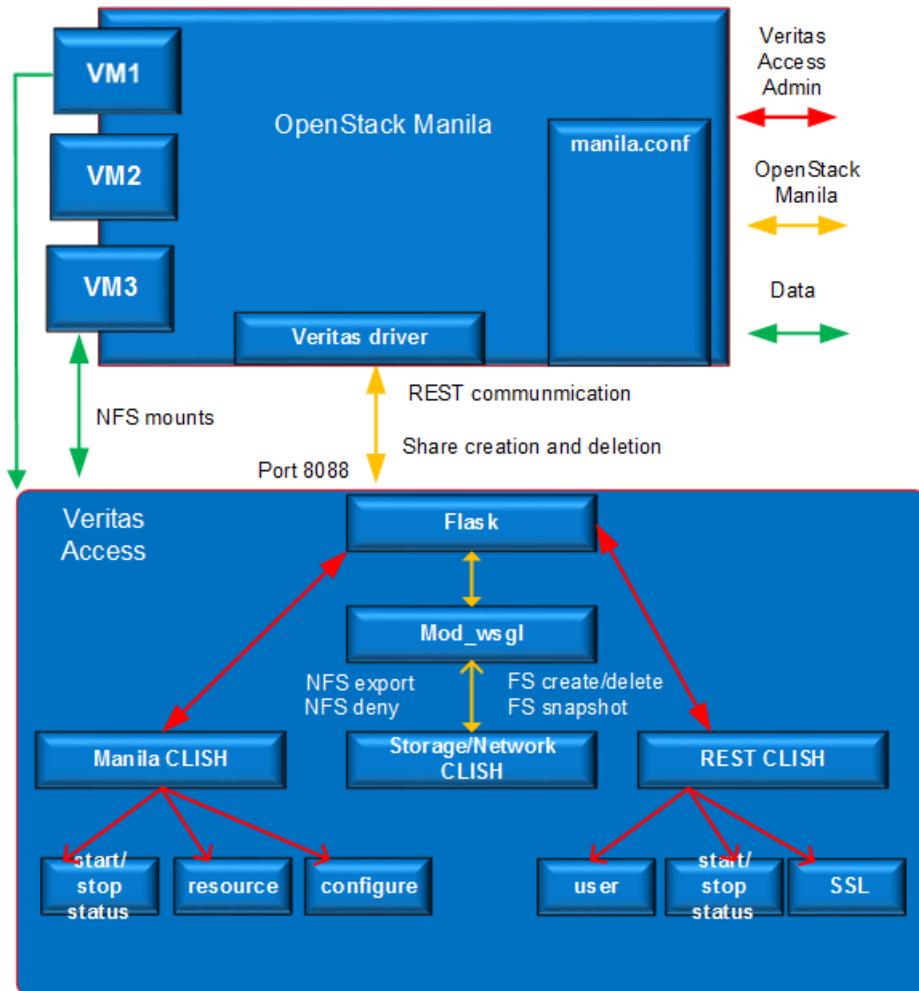
The OpenStack Manila driver communicates with Veritas Access using Representational State Transfer (REST) APIs, which provide access to resources (data entities) using HTTP or HTTPS, one at a time. By default, the REST server is configured for HTTP access only. Flask is the web application that is used to authenticate the Manila user and to run the OpenStack Manila driver.

The OpenStack Manila driver can create and manage simple file systems. For the backend to create simple file systems, use `isa_fstype=simple` in the `manila.conf` file.

Veritas Access REST APIs perform some of the following operations. This is not a complete list of the REST API operations.

- Create a REST user named Manila.
  - The Manila REST user is created during Veritas Access installation. There is no Veritas Access CLI command for creating the Manila REST user.
  - The OpenStack Manila driver authenticates with Veritas Access using Manila user credentials.
  - Veritas Access supports a single OpenStack tenant.
- Provide a mechanism for adding existing storage pools to the OpenStack Manila user.
  - The OpenStack Manila driver can create or delete file systems only from the storage pools that have been added through the appropriate REST operation. This prevents the OpenStack Manila driver from accidentally deleting the file system from any storage pools on Veritas Access.
  - You configure the added storage pools in the `manila.conf` file on the OpenStack controller node.
  - A single OpenStack Manila backend supports a single storage pool. If a second storage pool is required, another storage backend must be configured giving the details of the second storage pool. The second storage pool must be added to the Manila user using the appropriate command.

**Figure 15-1** OpenStack Manila architecture



## OpenStack Manila use cases

From the OpenStack controller node, an OpenStack administrator can do the following:

- Create and delete file systems.
- Allow and deny file system access to specific virtual machines.
- Provide IP-based access control.

- Create and delete snapshots of the file system.
- Create a file system from a snapshot.
- Provide free space statistics.
- NFS-based access of the shares from the instances.

From the Veritas Access node, a Veritas Access administrator can do the following:

- Make sure all the OpenStack Manila resources are started or stopped.
- Display the OpenStack Manila user
- Change the password of the OpenStack Manila user.
- Add and remove pools for the OpenStack Manila user.
- Display the pools and file systems available on the OpenStack controller node.
- Start the REST server.
- Display the status of the REST server.
- Set the certificate of the REST server.
- Enable the SSL of the REST server.
- Change the user password of the REST server.

## Configuring Veritas Access to work with OpenStack Manila

To configure OpenStack Manila for Veritas Access, perform the tasks in the order listed in [Table 15-1](#).

**Table 15-1** Tasks for configuring Veritas Access to work with OpenStack Manila

Task	Where to find more information
Start the REST server	See <a href="#">“Starting, stopping, or displaying the status of the REST server”</a> on page 271.
Display the status of the REST server	See <a href="#">“Starting, stopping, or displaying the status of the REST server”</a> on page 271.
Set the certificate of the REST server	See <a href="#">“Setting the certificate of the REST server”</a> on page 272.

**Table 15-1** Tasks for configuring Veritas Access to work with OpenStack Manila (*continued*)

Task	Where to find more information
Enable the secure Sockets Layer (SSL) of the REST server	See <a href="#">“Enabling or disabling the SSL status of the REST server”</a> on page 272.
Change the user password of the REST server	See <a href="#">“Changing the user password of the REST server”</a> on page 273.
Make sure all the OpenStack Manila resources are started	See <a href="#">“Starting, stopping, or displaying the status of the OpenStack Manila service”</a> on page 273.
Verify that the NFS and the REST services are started	See <a href="#">“Starting, stopping, or displaying the status of the REST server”</a> on page 271.
Configure and manage storage pools for the Manila user	See <a href="#">“Configuring and managing storage pools for the OpenStack Manila user”</a> on page 275.
Add the OpenStack Manila driver	See <a href="#">“Adding the OpenStack Manila driver”</a> on page 276.
Display the pools and file systems available on the OpenStack controller node	See <a href="#">“Configuring and managing storage pools for the OpenStack Manila user”</a> on page 275.
Create a new share backend	See <a href="#">“Creating a new share backend on the OpenStack controller node”</a> on page 277.
Restart the OpenStack Manila driver on the OpenStack controller node	See <a href="#">“Restarting the OpenStack Manila driver on the OpenStack controller node”</a> on page 278.
Create a share type	See <a href="#">“Creating an OpenStack Manila share type”</a> on page 280.
Create an OpenStack Manila file share	See <a href="#">“Creating an OpenStack Manila file share”</a> on page 281.
Create an OpenStack Manila snapshot	See <a href="#">“Creating an OpenStack Manila share snapshot”</a> on page 284.

## Starting, stopping, or displaying the status of the REST server

### To start the REST server

- ◆ Start the REST server.

```
System> webservices server start
```

For example:

```
System> webservices server start  
ACCESS REST SUCCESS V-288-1397 REST server start.
```

```
System> webservices server start  
ACCESS REST SUCCESS V-288-1397 REST server is running.
```

### To stop the REST server

- ◆ Stop the REST server.

```
System> webservices server stop
```

For example:

```
System> webservices server stop  
ACCESS REST SUCCESS V-288-1397 REST server stop.
```

```
System> webservices server stop  
ACCESS REST SUCCESS V-288-1397 REST server is not running.
```

### To display the status of the REST server

- ◆ Display the status of the REST server.

```
System> webservices server status
```

For example:

```
System> webservices server status  
REST Server: http://10.200.114.252:8088  
Certificate: /opt/SYMCsnas/conf/ssl.pem  
User: manila  
SSL: disable  
Status: ONLINE
```

## Setting the certificate of the REST server

Currently, Veritas Access uses a default certificate, which can be found in the following location: `/opt/SYMCsnas/scripts/system/rest.pem`. This certificate is generated by the Red Hat Enterprise Linux (RHEL) operating system; it is not an official certificate. If you want to use the official certificate for the REST server, you should upload the REST server certificate to all the nodes of Veritas Access, and set the path and name of the certificate using the `System> webservices SSL certificate` command.

This command is used only for HTTPS.

### To set the certificate of the REST server

- ◆ Set the certificate of the REST server.

```
System> webservices SSL certificate [certificate_full_path]
```

where *certificate\_full\_path* is the full path name where the SSL certificate is located.

For example:

```
System> webservices SSL certificate /opt/SYMCsnas/conf/ssl.pem  
ACCESS REST SUCCESS V-288-1397 Set REST server certificate successfully.
```

## Enabling or disabling the SSL status of the REST server

When SSL is disabled, HTTP is used, and when SSL is enabled, HTTPS is used. You have to change the `isa_ssl` flag in the `manila.conf` file on the OpenStack controller node. If SSL is disabled, you need to change the entry in the file to `isa_ssl = False`. If SSL is enabled, you need to change the entry to `isa_ssl = True`.

### To enable the SSL status of the REST server

- ◆ Enable the SSL status of the REST server.

```
System> webservices SSL enable
```

For example:

```
System> webservices SSL enable  
ACCESS REST SUCCESS V-288-1397 REST server SSL enabled.
```

### To disable the SSL status of the REST server

- ◆ Disable the SSL status of the REST server.

```
System> webservices SSL disable
```

For example:

```
System> webservices SSL disable  
ACCESS REST SUCCESS V-288-1397 REST server SSL disabled.
```

## Changing the user password of the REST server

### To change the user password of the REST server

- ◆ Change the password of the REST server.

```
System> webservices user password
```

For example:

```
System> webservices 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.
```

## Starting, stopping, or displaying the status of the OpenStack Manila service

The OpenStack Manila service depends on NFS and the web services.

---

**Note:** Starting and stopping the OpenStack Manila service and the REST server impacts OpenStack Manila server connectivity with Veritas Access. Any running operations during this time are affected.

---

### To start the OpenStack Manila service

- ◆ Start the OpenStack Manila service.

```
OPENSTACK> manila service start
```

This command starts the REST server and the NFS server.

For example:

```
OPENSTACK> manila service start
Success.
ACCESS manila SUCCESS V-288-999 OpenStack Manila service started
```

### To stop the OpenStack Manila service

- ◆ Stop the OpenStack Manila service.

```
OPENSTACK> manila service stop [force]
```

For example:

```
OPENSTACK> manila service stop
ACCESS manila ERROR V-288-999 There are NFS shares exported by Manila.
Either delete all the NFS exports or use the force option.
access_manila.OPENSTACK> manila service stop force
ACCESS manila WARNING V-288-999 OpenStack instances will continue to
access any
exported shares. No new share
creations/access will be allowed from OpenStack
Do you want to proceed (y/n): y
ACCESS manila SUCCESS V-288-999 OpenStack Manila service stopped
ACCESS_manila.OPENSTACK> manila service status
Manila service Status : OFFLINE
```

You would use the force option if you want to forcibly stop the OpenStack Manila service, even though there are existing NFS shares on OpenStack Manila pools.

If there are existing NFS shares from pools that are exported to OpenStack Manila, the `OPENSTACK> manila service stop` command fails.

For example:

```
ACCESS manila ERROR V-288-999 There are NFS shares exported by Manila.
Either delete all the NFS exports or use the force option.
```

**To display the status of the OpenStack Manila service**

- ◆ Display the status of the OpenStack Manila service.

```
OPENSTACK> manila service status
```

For example:

```
OPENSTACK> manila service status
Manila service Status : ONLINE
```

## Configuring and managing storage pools for the OpenStack Manila user

You create storage pools using the `Storage> pool create` command. Once the storage pool is created, then you can export the storage pool in OpenStack Manila.

**To export or unexport the storage pools to OpenStack Manila**

- 1 To export an existing storage pool to OpenStack Manila.

```
OPENSTACK> manila resource export pool_name
```

- 2 To unexport an existing storage pool provided to OpenStack Manila

```
OPENSTACK> manila resource delete pool_name
```

After unexporting the storage pools provided to OpenStack Manila, OpenStack Manila will not be able to create or delete any file systems from the unexported storage pool.

For example:

```
OPENSTACK> manila resource delete pool1
ACCESS REST SUCCESS V-288-1397 Removing exported pool pool1 from
REST server.
```

**To display the list of file systems and storage pools available for the OpenStack Manila user**

- ◆ Display the list of file systems and storage pools available for the OpenStack Manila user.

```
OPENSTACK> manila resource list
```

For example:

```
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:
10.1.12.9:/vx/0B54F556-ACE40746
10.1.12.1:/vx/0B54F556-ACE40746
```

**To display the configuration options that need to be performed on the OpenStack controller node for configuring Veritas Access storage pools**

- ◆ Display the configuration options that need to be performed on the OpenStack controller node to configure Veritas Access storage pools.

```
OPENSTACK> manila configure pool_name
```

## Adding the OpenStack Manila driver

The OpenStack Manila driver, `veritas_isa.py`, is responsible for the communication between the OpenStack host and the Veritas Access server. You can find the OpenStack Manila driver on the Veritas Access server at the following location:

`/opt/SYMCsnas/scripts/OpenStack`. You need to copy the OpenStack Manila driver, `veritas_isa.py`, on to the OpenStack host at the following location:

`/opt/stack/manila/manila/share/drivers`.

For example:

```
scp /opt/SYMCsnas/scripts/OpenStack/veritas_isa.py user@<OpenStack IP>:
/opt/stack/manila/manila/share/drivers
```

where `user` is the DevStack user.

To add the OpenStack Manila driver to the OpenStack RDO release, use the following location:

```
/usr/lib/python2.7/site-packages/manila/share/drivers/veritas_isa.py
```

## Creating a new share backend on the OpenStack controller node

A backend is an instance of the OpenStack Manila share service, which is defined in a section of the `manila.conf` file. Each backend has exactly one driver.

To create a new share backend `isa-share1` in OpenStack Manila, make the following changes on the OpenStack controller node, and restart the OpenStack Manila driver.

### To create a new share backend on the OpenStack controller node

- 1 On the OpenStack controller node, add the following configuration entries in the OpenStack Manila `/etc/manila/manila.conf` file.
  - In the `DEFAULT` section, add the following:

```
#####  
enabled_share_backends=isa-share1  
#####
```

If the entry `generic1` is already there, add the `isa-share1` entry after a comma. For example:

```
enabled_share_backends = generic1,isa-share1
```

- At the end of all sections in the `/etc/manila/manila.conf` file, add the following configuration entries:

```
#####  
[isa-share1]  
share_driver= manila.share.drivers.veritas_isa.VeritasShareDriver  
driver_handles_share_servers = False  
share_backend_name = isa-share1  
isa_server_ip = 10.182.96.179  
isa_port = 8088  
isa_ssl = False  
isa_fstype = simple  
isa_user = manila  
isa_pwd = password  
isa_pool = pool1  
#####
```

The following table describes the options.

<code>share_backend_name</code>	Name of the share backend. This name can be different for each share backend.
<code>share_driver</code>	OpenStack Manila driver name.
<code>isa_server_ip</code>	Console IP address of the Veritas Access cluster.
<code>isa_port</code>	8088  The port on Veritas Access to which the Manila driver is connected.
<code>isa_ssl</code>	SSL certificate on the REST server.
<code>isa_fstype</code>	Type of file system to be created on the specified pool. It can be <code>simple</code> .
<code>isa_user</code>	REST user name.
<code>isa_pwd</code>	REST password.
<code>isa_pool</code>	Existing storage pool on Veritas Access from which the file systems are to be created.

You use the `OPENSTACK> manila configure` command to display the configuration options that need to be performed on the OpenStack controller node.

See [“Configuring and managing storage pools for the OpenStack Manila user”](#) on page 275.

## 2 Restart the OpenStack Manila services.

The restart is on the OpenStack controller node, not on Veritas Access.

See [“Restarting the OpenStack Manila driver on the OpenStack controller node”](#) on page 278.

## Restarting the OpenStack Manila driver on the OpenStack controller node

The Veritas Access OpenStack Manila driver can be restarted from the OpenStack screen console. The screen console on the OpenStack controller node can be invoked in the following ways.

**To find the instance of the OpenStack screen login as the DevStack user**

- 1** Find the instance of the OpenStack screen login as the DevStack user.

```
[staker@Manila /]$ screen -ls
There is a screen on:
      25577.stack      (Detached)
1 Socket in /var/run/screen/S-staker
```

- 2** Run `screen -r screen_name` to get the screen console.

```
[staker@Manila /]$ screen -r 25577.stack
```

- 3** On the screen console, confirm the following sections are visible:

```
m-api, m-shr, m-sch*
```

You can navigate to these sections using the following keys on the keyboard:

Ctrl + a + n            To move toward the right-hand side.

Ctrl + a + p            To move toward the left-hand side.

`m-api`, `m-shr`, and `m-sch` are the OpenStack Manila related services. You can restart these services individually by moving to the screen console and using `Ctrl + c`. `Ctrl + c` terminates these sessions. Use the Up Arrow key and press Enter to restart the driver. It is advisable to restart all three services, `m-api`, `m-shr`, and `m-sch`.

For example, to restart `m-api` after pressing `Ctrl + c` and the Up Arrow key, you may see the following command:

```
[staker@Manila devstack]$ cd /opt/stack/manila && /usr/bin/manila-api --config-file
/etc/manila/manila.conf & echo $! >/opt/stack/status/stack/m-api.pid; fg || echo "m-api failed
to start" | tee "/opt/stack/status/stack/m-api.failure"
```

- 4 Press `Enter` again to start the service.
- 5 If you are using OpenStack RDO, use the following steps to restart the Veritas OpenStack Manila driver.

Login to the OpenStack controller node.

For example:

```
source /root/keystonerc_admin
```

Restart the OpenStack Manila services.

```
openstack-service restart openstack-manila-api
```

```
openstack-service restart openstack-manila-scheduler
```

```
openstack-service restart openstack-manila-share
```

For more information, refer to the *Openstack Administration Guide*.

In the OpenStack RDO Kilo release, you can review the OpenStack Manila logs at:

```
/var/log/manila/
```

## Creating an OpenStack Manila share type

An OpenStack Manila share type is an administrator-defined type of service that is used by the Manila scheduler to make scheduling decisions. OpenStack tenants can list share types and then use them to create new shares.

### To create an OpenStack Manila share type

- ◆ On the OpenStack controller node, create a share type for `isa-backend1` and `isa_backend2`.

```
manila@C4110-R720xd-111045:~/OpenStack$ manila type-create isa-backend1  
False
```

### To associate the share type to a share backend

- ◆ On the OpenStack controller node, associate the share type to a share backend.

```
manila@C4110-R720xd-111045:~/OpenStack$ manila type-key isa-backend1 set  
driver_handles_share_servers=false share_backend_name=isa-share1  
manila@C4110-R720xd-111045:~/OpenStack$ manila type-key isa-backend2  
set driver_handles_share_servers=false share_backend_name=isa-share2
```

## Creating an OpenStack Manila file share

An OpenStack Manila file share is equivalent to a file system in Veritas Access. You can create an OpenStack Manila file share on the OpenStack controller node.

---

**Note:** Due to a REST limitation, you cannot create or delete more than five file systems in parallel using the OpenStack Manila GUI.

---

**To create an OpenStack Manila file share on the OpenStack controller node**

- 1 On the OpenStack controller node, if you wanted to create two OpenStack Manila file shares called `prod_fs` and `finance_fs` of size 1 GB accessible over NFS, enter the following:

One of the file shares resides on `isa_backend1`, and one of the file shares resides on `isa-backend2`.

```
manila@C4110-R720xd-111045:~/OpenStack$ manila create --name prod_fs
--share-type isa-backend1 NFS 1
```

```
manila@C4110-R720xd-111045:~/OpenStack$ manila create --name finance_fs
--share-type isa-backend2 NFS 1
```

Use the `manila list` command to see how the file shares look on the OpenStack controller node.

You can see how the file systems look on Veritas Access as part of the share creation process.

Storage> fs list	FS	STATUS	SIZE	LAYOUT	MIRRORS	COLUMNS	USE%	NFS	SHARED	CIFS	SHARED	FTP	SHARED	SECONDARY	TIER	POOL	LIST
	CB94D066-61977D6A	online	1.00G	simple	-	-	6%	no	no	no	no						pool2
	C491EFE6-5A0484C0	online	1.00G	simple	-	-	6%	no	no	no	no						pool1

## 2 Give `prod_fs` read-write access to 10.182.111.84.

```
manila@C4110-R720xd-111045:~/OpenStack$ manila access-allow --access-level rw
ecba1f14-86b0-4460-a286-a7e938162fb4 ip 10.182.111.84
```

```

+-----+-----+
| Property | Value |
+-----+-----+
| share_id | ecba1f14-86b0-4460-a286-a7e938162fb4 |
| deleted  | False |
| created_at | 2015-04-28T17:59:45.514849 |
| updated_at | None |
| access_type | ip |
| access_to | 10.182.111.84 |
| access_level | rw |
| state | new |
| deleted_at | None |
| id | 8alc2d0b-a3fc-4405-a8eb-939adb8799db |
+-----+-----+

```

In the `manila access-allow` command, you can get the ID (`ecba1f14-86b0-4460-a286-a7e938162fb4`) from the output of the `manila list` command.

## 3 Give `finance_fs` read-write access to 10.182.111.81.

```
manila@C4110-R720xd-111045:~/OpenStack$ manila access-allow --access-level rw
f8da8ff6-15e6-4e0c-814b-d6ba8d08543c ip 10.182.111.81
```

```

+-----+-----+
| Property | Value |
+-----+-----+
| share_id | f8da8ff6-15e6-4e0c-814b-d6ba8d08543c |
| deleted  | False |
| created_at | 2015-04-28T18:01:49.557300 |
| updated_at | None |
| access_type | ip |
| access_to | 10.182.111.81 |
| access_level | rw |
| state | new |
| deleted_at | None |
| id | ddcfc2d2-7e71-443a-bd94-81ad05458e32 |
+-----+-----+

```

```
manila@C4110-R720xd-111045:~/OpenStack$ manila access-list
ecba1f14-86b0-4460-a286-a7e938162fb4root@finance:~$
```

## Creating an OpenStack Manila share snapshot

You can create an OpenStack Manila share snapshot, which is equivalent to creating a snapshot (checkpoint) in Veritas Access. Creating an OpenStack Manila share snapshot creates a checkpoint of the specific file system on Veritas Access. The checkpoint that is created is non-removable.

Deleting a snapshot deletes the checkpoint of that file system.

### To create an OpenStack Manila share snapshot

- ◆ On the OpenStack controller node, if you want to create `fin_snap` and `prod_snap` snapshots, enter the following:

```
manila@C4110-R720xd-111045:~/OpenStack$ manila snapshot-create --name fin_snap  
d3ab5cdc-4300-4f85-b4a5-e2a55d835031
```

```
manila@C4110-R720xd-111045:~/OpenStack$ manila snapshot-create --name prod_snap  
2269b813-0031-419e-a2d3-0073cdb2776e
```

Use the `manila snapshot-list` command to display the snapshots you created.

## Creating an OpenStack Manila share from an OpenStack Manila share snapshot

You can create an OpenStack Manila share from an OpenStack Manila share snapshot

### To create an OpenStack Manila share from an OpenStack Manila share snapshot

- ◆ On the OpenStack controller node, if you want to create an OpenStack Manila share from an OpenStack Manila share snapshot `prod_snap`, enter:

```
manila@C4110-R720xd-111045:~/OpenStack$ manila create --name prod_snap_fs  
--snapshot-id 5d695533-ba28-4be2-bcd0-b87319591e46 NFS 1
```

Use the `manila list` command to display the share you created from the snapshot.

# Configuring Veritas Access to work with Oracle Direct NFS

This chapter includes the following topics:

- [About using Veritas Access with Oracle Direct NFS](#)
- [About the Oracle Direct NFS architecture](#)
- [Best practices for improving Oracle database performance](#)
- [About Oracle Direct NFS node or storage connection failures](#)
- [Configuring an Oracle Direct NFS storage pool](#)
- [Configuring an Oracle Direct NFS file system](#)
- [Configuring an Oracle Direct NFS share](#)

## About using Veritas Access with Oracle Direct NFS

Veritas Access lets you create and manage storage for Oracle database clients. Oracle hosts access the storage using Oracle Direct NFS (DNFS).

Oracle Direct NFS is an optimized NFS (Network File System) client that provides faster access to NFS storage that is located on NAS storage devices. The Oracle Database Direct NFS client integrates the NFS client functionality directly in the Oracle software. Through this integration, the I/O path between Oracle and the NFS server is optimized, providing significantly better performance. In addition, the Oracle

Direct NFS client simplifies and, in many cases, automates the performance optimization of the NFS client configuration for database workloads.

The Oracle Direct NFS client outperforms traditional NFS clients, and is easy to configure. The Oracle Direct NFS client provides a standard NFS client implementation across all hardware and operating system platforms.

Veritas Access creates different storage pools for different Oracle object types. Veritas Access has the following storage pools as described in [Table 16-1](#).

**Table 16-1** Veritas Access storage pools for Oracle object types

Pool Name	Database Object Type	Function
<code>ora_data_pool</code>	Oracle TABLE data files	Stores TABLE data of data files.  This database object type uses striped volumes over four LUNs. The stripe size is 256K.
<code>ora_index_pool</code>	Oracle INDEX files	Stores INDEX data.
<code>ora_temp_pool</code>	Temporary files	Stores temporary files.  The storage administrator should make sure the LUNs are from the fastest tier. Temporary files are used for sort, merge, or join queries.
<code>ora_archive_pool</code>	Archive logs	Stores archive logs.  This database object type is a concatenated volume. Tier 2 LUNs can be used for this storage pool.
<code>ora_tnxlog_pool</code>	REDO txnlog files	Stores REDO transaction logs.  It is recommended to assign the fastest storage LUNs to this storage pool.

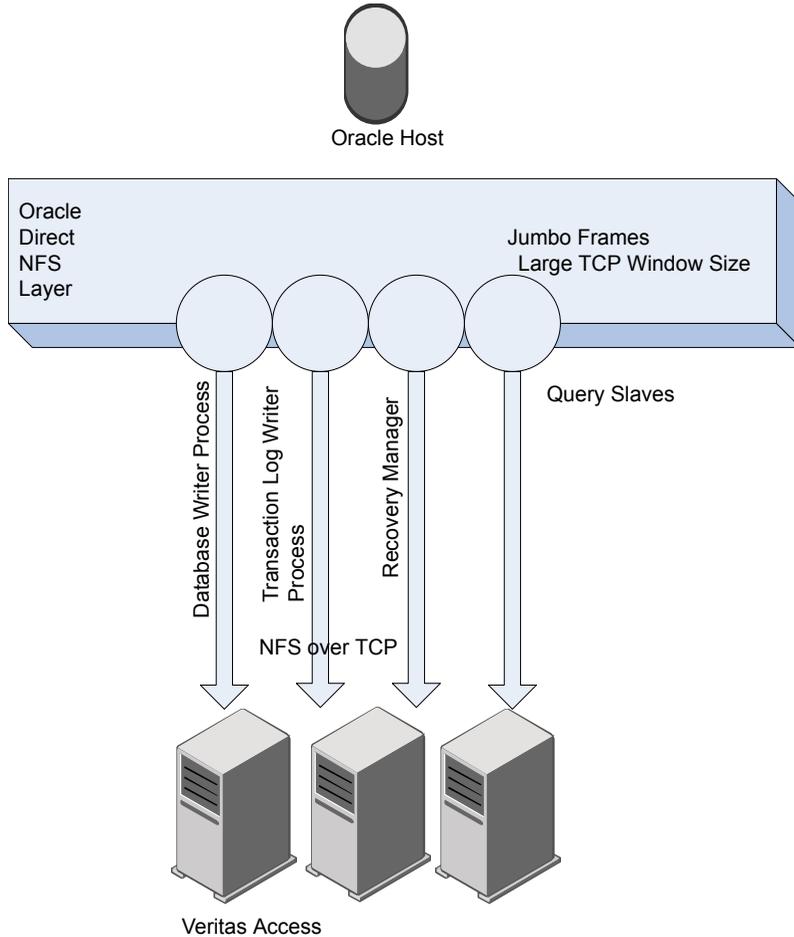
## About the Oracle Direct NFS architecture

Oracle Direct NFS can issue 1000s of concurrent operations due to the parallel architecture. Every Oracle process has its own TCP connection.

See the *Veritas Access Installation Guide* for the supported Oracle operating systems.

Figure 16-1 describes the data flow from the Oracle host to Veritas Access.

**Figure 16-1** Oracle Direct NFS architecture



Setting a larger frame size on an interface is commonly referred to as using jumbo frames. Jumbo frames help reduce fragmentation as data is sent over the network and in some cases, can also provide better throughput and reduced CPU usage.

You can configure jumbo frames for Oracle Direct NFS by setting the Maximum Transmission Unit (MTU) value.

See [“Configuring Ethernet interfaces”](#) on page 56.

# Best practices for improving Oracle database performance

Oracle database performance depends on I/O bandwidth and latency.

The Oracle database has the following object types:

- DATA
- INDEX
- TXNLOG
- ARCHLOG
- TEMPFILES

See [“About using Veritas Access with Oracle Direct NFS”](#) on page 285.

The Oracle database transaction rate depends heavily on TXNLOG write latency.

**Table 16-2** Best practices for improving Oracle database performance

Item	Action
DATA and INDEX files	Separate DATA and INDEX files into separate disk pools with a minimum of four LUNs.
REDOLOG files	Configure REDOLOG files in a separate file system (NFS share). The underlying storage LUNs should not be shared with other volumes or file systems.
TEMPFILES	For data warehouse applications, keep TEMPFILES in separate pools with a minimum of four LUNs.
TXNLOG files	Place TXNLOG files in a separate disk pool with dedicated fast LUNs.
NFS daemon threads	To get better performance, increase NFS daemon threads to 128 or more. If the network permits, you may want to enable jumbo frames.  See <a href="#">“About the Oracle Direct NFS architecture”</a> on page 286.
Veritas Access database-specific file systems	Access Veritas Access database-specific file systems from the Oracle host using dedicated virtual IPs. Do not use the same virtual IP for other applications.

**Table 16-2** Best practices for improving Oracle database performance  
*(continued)*

Item	Action
Veritas Access file systems	<p>Always use Oracle recommended mount options to mount Veritas Access file systems on the Oracle host. This mount option depends on the Oracle database version.</p> <p>See the <i>Veritas Access Installation Guide</i> for the supported Oracle database versions.</p> <p>See the Oracle documentation for the recommended mount options.</p>

## About Oracle Direct NFS node or storage connection failures

When a node or a storage connection fails, Veritas Access fails over the virtual IP (VIP) to the healthy node. If Oracle does active transactions, some I/O can fail during this VIP failover time window. Oracle generally issues several asynchronous I/O requests using Oracle Direct NFS in parallel. If Oracle detects some I/O failure waiting for completed I/Os, the result depends on the database file type. If the write fails for the REDO transaction log or the database control files, then the database instance fails. If I/O to a data file fails, then that particular data file is taken offline. The SYSTEM and the UNDO data files are considered critical data files. The Oracle database fails if I/O to these critical data files fail. When the database instance fails, the database administrator should wait until the VIP fails over to the healthy Veritas Access node. When the VIP is online, the database administrator can start up the database and then recover the database.

## Configuring an Oracle Direct NFS storage pool

### To create an Oracle Direct NFS storage pool

- ◆ Use the `Database> pool create` command to create a pool to store database objects.

```
Database> pool create obj-type disk1[,disk2,...]
```

*obj-type*

Specifies the Oracle object type.

It is recommended to group the storage according to the database objects that are stored in the file system. Oracle database objects are broadly divided into REDO transaction logs, archived logs, table data, index, or temporary files.

Available values include:

- txnlog
- data
- index
- temp
- archivelog

See [“About using Veritas Access with Oracle Direct NFS”](#) on page 285.

*disk1, disk2*

Specifies the disks to include in the Oracle Direct NFS storage pool.

An error message displays if a disk is not present, or if the disk is already used.

For example:

```
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
```

### To destroy an Oracle Direct NFS storage pool

- ◆ To destroy a specified Oracle Direct NFS storage pool, enter the following:

```
Database> pool destroy obj-type
```

For example:

```
Database> pool destroy data
```

**To list all your Oracle Direct NFS storage pools**

- ◆ Use the `Database> pool list` command to list all your Oracle Direct NFS storage pools that are configured for the database.

```
Database> pool list
POOL NAME          DISKS
-----          -
ora_DATA_pool      vmdk0_1 vmdk0_2
ora_TXNLOG_pool    vmdk0_3
ora_ARCHIVE_pool   vmdk0_4
ora_INDEX_pool     vmdk0_5,vmdk0_6
```

# Configuring an Oracle Direct NFS file system

**To create an Oracle Direct NFS file system**

- ◆ Use the `Database> fs create` command to create an Oracle Direct NFS file system for storing objects.

```
Database> fs create obj-type db_name fs_name size
```

*obj-type*

Specifies the Oracle object type.

Available values include:

- txnlog
- data
- index
- temp
- archivelog

See [“About using Veritas Access with Oracle Direct NFS”](#) on page 285.

*db\_name*

Specifies the Oracle database name.

*fs\_name*

Specifies the file system name for which you want to create.

For a given database, Veritas recommends having at least three file systems provisioned from respective storage pools:

- One file system for txnlog
- One file system for data
- One file system for archivelog

*size* Specifies the size of the file system that you want to create.

For example:

```
Database> fs create data tpcc_data1 300g
Database> fs create txnlog tpcc_redo1 12g
Database> fs create index tpcc_indx1 48g
Database> fs create archiveolog tpcc_arch1 100g
```

### To destroy an Oracle Direct NFS file system

- ◆ Use the `Database> fs destroy` command to destroy an Oracle Direct NFS file system.

```
Database> fs destroy db_name fs_name
```

For example:

```
Database> fs destroy tpcc data_fs
```

### To list the Oracle Direct NFS file systems

- ◆ Use the `Database> fs list` command to list the Oracle Direct NFS file systems that are created for storing database files.

```
Database> fs list
```

## Configuring an Oracle Direct NFS share

### To configure an Oracle Direct NFS share

- 1 Use the `Database> share add` command to share and export a file system. After issuing the `Database> share add` command, database clients are able to NFS mount the specified file system on their Oracle host.

```
Database> share add obj-type export_dir [client]
```

<i>obj_type</i>	Specifies the Oracle object type. Available values include: <ul style="list-style-type: none"><li>■ txnlog</li><li>■ data</li><li>■ index</li><li>■ temp</li><li>■ archivelog</li></ul> See <a href="#">“About using Veritas Access with Oracle Direct NFS”</a> on page 285.
<i>export_dir</i>	Specifies the directory location of the exported file system.
<i>client</i>	Specifies the database client.

For example:

```
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
```

- 2 Use the `Database> share show` command to display all the shared database file systems.

```
Database> share show
```

- 3 Use the `Database> share delete` command to delete or unshare the exported file system.

```
Database> share delete export-dir [client]
```

# Monitoring and troubleshooting

- [Chapter 17. Monitoring events and logs](#)
- [Chapter 18. Displaying statistics](#)
- [Chapter 19. Using the locally saved configuration files](#)
- [Chapter 20. Veritas Access tuning](#)

# Monitoring events and logs

This chapter includes the following topics:

- [About configuring event notifications](#)
- [About severity levels and filters](#)
- [Configuring an email group](#)
- [Configuring a syslog server](#)
- [Displaying events on the console](#)
- [About SNMP notifications](#)
- [Configuring an SNMP management server](#)
- [Configuring events for event reporting](#)
- [Exporting events in syslog format to a given URL](#)

## About configuring event notifications

Veritas Access monitors the status and health of various network and storage components, and generates events to notify the administrator. Veritas Access provides a mechanism to send these events to external event monitoring applications like syslog server, SNMP trap logger, and mail servers. This section explains how to configure Veritas Access so that external event monitoring applications are notified of events on the Veritas Access cluster.

## About severity levels and filters

Veritas Access monitors events of different severity levels. Set the severity to a particular level to specify the severity level to include in notifications. Notifications are sent for events having the same or higher severity.

Table 17-1 describes the valid Veritas Access severity levels in descending order of severity.

**Table 17-1** Severity levels

Valid value	Description
emerg	Indicates that the system is unusable
alert	Indicates that immediate action is required
crit	Indicates a critical condition
err	Indicates an error condition
warning	Indicates a warning condition
notice	Indicates a normal but a significant condition
info	Indicates an informational message
debug	Indicates a debugging message

Veritas Access also classifies event notifications by type. Set the event filter to specify which type of events to include in notifications. Notifications are sent only for events matching the given filter.

The filter is set to one of the following options:

- Network - for networking events
- Storage - for storage-related events. For example, events related to file systems, snapshots, disks, and pools.
- All - resets the filter to show all events.

For example, if the filter is set to `network`, a network event triggers a notification. A storage-related event would not trigger a notification.

## Configuring an email group

Veritas Access can be configured to send email messages to users or groups of users through an external SMTP server.

### To display attributes of an email group

- ◆ To display attributes of an email group, enter the following:

```
Report> email show [group]
```

where *group* is optional, and it specifies the group for which to display the attributes. If the specified group does not exist, an error message is displayed. For example:

```
Report> email show root
Group Name: root
Severity of the events: info,debug
Filter of the events: all,storage
Email addresses in the group: user@hostname.domain.name
OK Completed
```

### To add a new email group

- ◆ To add a new email group, enter the following:

```
Report> email add group group
```

where *group* specifies the name of the new email group and can only contain the following characters:

- Alpha characters
- Numbers
- Hyphens
- Underscores

If the entered group already exists, then no error message is displayed. For example:

```
Report> email add group alert-grp
OK Completed
```

Multiple email groups can be defined, each with their own email addresses, event severity, and filter.

### To add an email address to an existing group

- ◆ To add an email address to an existing group, enter the following:

```
Report> email add email-address group email-address
```

For example:

```
Report> email add email-address alert-grp username@company.com  
OK Completed
```

group	Specifies the group to which the email address is added. The email group must already exist.
email-address	Specifies the email address to be added to the group.

### To add a severity level to an existing email group

- ◆ To add a severity level to an existing email group, enter the following:

```
Report> email add severity group severity
```

For example:

```
Report> email add severity alert-grp alert  
OK Completed
```

group	Specifies the email group for which to add the severity. The email group must already exist.
severity	Indicates the severity level to add to the email group. See <a href="#">“About severity levels and filters”</a> on page 296. Only one severity level is allowed at one time. You can have two different groups with the same severity levels and filters. Each group can have its own severity definition. You can define the lowest level of the severity that triggers all other severities higher than it.

### To add a filter to an existing group

- ◆ To add a filter to an existing group, enter the following:

```
Report> email add filter group filter
```

**group** Specifies the email group for which to apply the filter. The email group must already exist.

**filter** Specifies the filter for which to apply to the group. See [“About severity levels and filters”](#) on page 296. The default filter is `all`.

A group can have more than one filter, but there may not be any duplicate filters for the group.

For example:

```
Report> email add filter root storage  
OK Completed
```

### To delete an email address from an existing group

- ◆ To delete an email address from an existing group, enter the following:

```
Report> email del email-address group email-address
```

**group** Specifies the group from which to delete the email address.

**email-address** Specifies the email address from which to delete from the group.

For example, to delete an existing email address from the email group, enter the following:

```
Report> email del email-address root testuser@localhost
```

**To delete a filter from an existing group**

- ◆ To delete a filter from an existing group, enter the following:

```
Report> email del filter group filter
```

*group* Specifies the group to remove the filter from.

*filter* Specifies the filter to be removed from the group.

See [“About severity levels and filters”](#) on page 296.

The default filter is *all*.

**To delete an existing email group**

- ◆ To delete an existing email group, enter the following:

```
Report> email del group group
```

where *group* specifies the name of the email group to be deleted.

**To delete a severity from a specified group**

- ◆ To delete a severity from a specified group, enter the following:

```
Report> email del severity group severity
```

*group* Specifies the name of the email group from which the severity is to be deleted.

*severity* Specifies the severity to delete from the specified group.

See [“About severity levels and filters”](#) on page 296.

**To display mail server settings**

- ◆ To display mail server settings, enter the following:

```
Report> email get  
E-Mail Server: smtp.veritas.com  
E-Mail Username: adminuser  
E-mail User's Password: *****  
OK Completed
```

### To add a mail server and user account

- ◆ To add a mail server and user account from which email notifications are sent out, enter the following:

```
Report> email set [email-server] [email-user]
```

email-server            Specifies the external mail server from which email notifications are sent out.

email-user             Specifies the user account from which email notifications are sent out.

If `email-user` is specified, then the password for that user on the SMTP server is required.

For example:

```
Report> email set smtp.veritas.com adminuser  
Enter password for user 'adminuser': *****
```

### To delete the mail server from sending email messages

- ◆ To delete the mail server from sending email messages, enter the following command without any options:

```
Report> email set
```

## Configuring a syslog server

Veritas Access can be configured to send syslog messages to syslog servers based on set severities and filters.

In Veritas Access, options include specifying the external system log (syslog) server for event reporting, and setting the filter and the severity levels for events. Event notifications matching configured severity levels and filters are logged to those external syslog servers.

See [“About severity levels and filters”](#) on page 296.

### To display the list of syslog servers

- ◆ To display the list of syslog servers, enter the following:

```
Report> syslog show
```

**To add a syslog server to receive event notifications**

- ◆ To add a syslog server to receive event notifications, enter the following:

```
Report> syslog add syslog-server-ipaddr
```

where *syslog-server-ipaddr* specifies the host name or the IP address of the external syslog server.

**To set the severity of syslog messages**

- ◆ To set the severity of syslog messages to be sent, enter the following:

```
Report> syslog set severity value
```

where *value* indicates the severity of syslog messages to be sent.

For example:

```
Report> syslog set severity warning
```

See [“About severity levels and filters”](#) on page 296.

**To set the filter level of syslog messages**

- ◆ To set the filter level of syslog messages to be sent, enter the following:

```
Report> syslog set filter value
```

where *value* indicates the filter level of syslog messages to be sent.

For example:

```
Report> syslog set filter storage  
OK Completed
```

See [“About severity levels and filters”](#) on page 296.

**To display the values of the configured filter and severity level settings**

- ◆ To display the values of the configured filter and severity level settings, enter the following:

```
Report> syslog get filter|severity
```

For example:

```
Report> syslog get severity  
Severity of the events: err  
OK Completed
```

### To delete a syslog server from receiving message notifications

- ◆ To delete a syslog server from receiving message notifications, enter the following:

```
Report> syslog delete syslog-server-ipaddr
```

*syslog-server-ipaddr* specifies the host name or the IP address of the syslog server.

## Displaying events on the console

### To display events on the console

- ◆ To display events on the console, enter the following:

```
Report> showevents [number_of_events]
```

where *number\_of\_events* specifies the number of events that you want to display. If you leave *number\_of\_events* blank, or if you enter **0**, Veritas Access displays all of the events in the system.

## About SNMP notifications

Simple Network Management Protocol (SNMP) is a network protocol to simplify the management of remote network-attached devices such as servers and routers. SNMP is an open standard system management interface. Information from the Management Information Base (MIB) can also be exported.

SNMP traps enable the reporting of a serious condition to a management station. The management station is then responsible for initiating further interactions with the managed node to determine the nature and extent of the problem.

See [“About severity levels and filters”](#) on page 296.

# Configuring an SNMP management server

## To add an SNMP management server to receive SNMP traps

- ◆ To add an SNMP management server to receive SNMP traps, enter the following:

```
Report> snmp add snmp-mgmtserver-ipaddr [community_string]
```

*snmp-mgmtserver-ipaddr* specifies the host name or the IP address of the SNMP management server.

[*community\_string*] specifies the community name for the SNMP management server. The default *community\_string* is `public`.

You can specify either an IPv4 address or an IPv6 address.

When you use the `Report> snmp show` command, *community\_string* displays as follows:

```
public@mgmtserv1.veritas.com, public@mgmtserv2.veritas.com
```

For example, if using the IP address, enter the following:

```
Report> snmp add 10.10.10.10
```

```
OK Completed
```

```
Report> snmp add 2001:21::11
```

```
Command completed successfully
```

For example, if using the host name, enter the following:

```
Report> snmp add mgmtserv1.veritas.com
```

```
OK Completed
```

SNMP traps can be sent to multiple SNMP management servers.

## To display the current list of SNMP management servers

- ◆ To display the current list of SNMP management servers, enter the following:

```
Report> snmp show
```

```
Configured SNMP management servers:
```

```
10.10.10.10,mgmtserv1.veritas.com
```

```
public@mgmtserv1.veritas.com, public@mgmtserv2.veritas.com
```

```
OK Completed
```

### To delete an already configured SNMP management server from receiving SNMP traps

- ◆ To delete an already configured SNMP management server from receiving SNMP traps, enter the following:

```
Report> snmp delete snmp-mgmtserver-ipaddr
```

*snmp-mgmtserver-ipaddr* specifies the host name or the IP address of the SNMP management server.

For example:

```
Report> snmp delete 10.10.10.10  
OK Completed
```

### To set the severity for SNMP traps to be sent

- ◆ To set the severity for SNMP traps to be sent, enter the following:

```
Report> snmp set severity value
```

where *value* indicates the severity for the SNMP trap to be sent.

For example:

```
Report> snmp set severity warning  
OK Completed
```

See [“About severity levels and filters”](#) on page 296.

### To set the filter level of SNMP traps

- ◆ To set the filter level for SNMP traps, enter the following:

```
Report> snmp set filter value
```

where *value* indicates the filter.

For example:

```
Report> snmp set filter network  
OK Completed
```

See [“About severity levels and filters”](#) on page 296.

**To display the filter or the severity levels of SNMP traps to be sent**

- ◆ To display the filter or the severity levels of SNMP traps to be sent, enter the following:

```
Report> snmp get filter|severity
```

For example:

```
Report> snmp get severity
Severity of the events: warning
OK Completed
Report> snmp get filter
Filter for the events: network
OK Completed
```

**To export the SNMP MIB file to a given URL**

- ◆ To export the SNMP MIB file to a given URL, enter the following:

```
Report> snmp exportmib url
```

where *url* specifies the location the SNMP MIB file is exported to.

FTP and SCP URLs are supported.

For example:

```
Report> snmp exportmib
scp://admin@server1.veritas.com:/tmp/access_mib.txt
Password: *****
OK Completed
```

If the *url* specifies a remote directory, the default file name is `access_mib.txt`.

# Configuring events for event reporting

## To reduce duplicate events

- ◆ To reduce the number of duplicate events that are sent for notifications, enter the following:

```
Report> event set dup-frequency number
```

where *number* indicates time (in seconds) in which only one event (of duplicate events) is sent for notifications.

For example:

```
Report> event set dup-frequency 120  
OK Completed
```

where *number* indicates the number of duplicate events to ignore.

```
Report> event set dup-number number
```

For example:

```
Report> event set dup-number 10  
OK Completed
```

## To display the time interval or the number of duplicate events sent for notifications

- ◆ To display the time interval, enter the following:

```
Report> event get dup-frequency
```

For example:

```
Report> event get dup-frequency  
Duplicate events frequency (in seconds): 120  
OK Completed
```

To set the number of duplicate events that are sent for notifications, enter the following:

```
Report> event get dup-number
```

For example:

```
Report> event get dup-number  
Duplicate number of events: 10  
OK Completed
```

### To set the time interval for scanning event notifications

- ◆ To set the time interval for scanning event notifications in `/var/log/messages` and `/var/log/messages-*.bz2` files, enter the following:

```
Report> event set log-scan-frequency frequency
```

where *frequency* is the time interval in seconds for scanning the `/var/log/messages` directory.

For example, to set the scan frequency to 30 seconds, enter the following:

```
Report> event set log-scan-frequency 30  
Command completed successfully
```

### To display the time interval for scanning event notifications

- ◆ To display the time interval for scanning event notifications, enter the following:

```
Report> event get log-scan frequency
```

For example:

```
Report> event get log-scan-frequency  
Log scan frequency (in seconds): 120 (default)  
Command completed successfully
```

### To set the from email address when sending email notifications to users

- ◆ To set the from email address when sending email notifications to users, enter the following:

```
Report> event set from-address from-email-address
```

where *from-email-address* is the from email address when sending email notifications to users.

For example, to set the from email address to `testaddr@veritas.com`, enter the following:

```
Report> event set from-address testaddr@veritas.com  
Command completed successfully
```

**To display the from email address when sending email notifications to users**

- ◆ To display the from email address when sending email notifications to users, enter the following:

```
Report> event get from-address
```

For example, to view the newly set from email address, enter the following:

```
Report> event get from-address  
Email from address: testaddr@veritas.com  
Command completed successfully
```

## Exporting events in syslog format to a given URL

You can export events in syslog format to a given URL.

Supported URLs for upload include:

- FTP
- SCP

**To export events in syslog format**

- ◆ To export events in syslog format to a given URL, enter the following:

```
Report> exportevents url
```

url Exports the events in syslog format to the specified URL. URL supports FTP and SCP. If the URL specifies the remote directory, the default file name is `access_event.log`.

For example:

```
Report> exportevents  
scp://root@server1.veritas.com:/exportevents/event.1  
Password: *****  
OK Completed
```

# Displaying statistics

This chapter includes the following topics:

- [Displaying cluster or node statistics](#)
- [Displaying file system I/O statistics](#)

## Displaying cluster or node statistics

The `system> stat` command displays the system, Dynamic Multi-Pathing (DMP), and process-related node-wide statistics. The load in the displayed output is the load from the last 1, 5, and 15 minutes.

**To display the system statistics**

- ◆ To display cluster wide or node-wide statistics, enter the following:

```
System> stat sys [node] | dmp [node] | all [node] | cluster | rdma [node]
```

sys	Displays the system-related statistics.
dmp	Displays the DMP-related statistics.
cluster	Displays the aggregate of the I/O and network performances from each node and averages out the number of nodes in the cluster to show the statistics at the cluster level. The variable <i>node</i> does not apply to this option.
all	Displays the system and DMP-related statistics of one node at a time in the cluster or all of the nodes in the cluster.
node	The name of the node in the cluster.
rdma	Display RDMA statistics of all the nodes or specific node(s) in the cluster at a time.

To view the cluster-wide network and I/O throughput, enter the following:

```
System> stat cluster
Gathering statistics...
Cluster wide statistics:::
=====
IO throughput :: 0
Network throughput :: 1.205
```

# Displaying file system I/O statistics

## To display file system I/O statistics

- ◆ To display file system I/O statistics, enter the following:

```
System> stat fsio [fsname]
```

where *fsname* is the name of the file system for which you want to display the file system I/O statistics.

```
System> stat fsio testfs1
```

NAME	OPERATIONS		BLOCKS		AVG TIME(ms)	
	READ	WRITE	READ	WRITE	READ	WRITE
Node: access1_0						
=====						
testfs1_tier1	532	206	2336	7486	1.17	9.98
testfs1_tier2	1	1	2	16	4.00	8.00
Node: access1_1						
=====						
testfs1_tier1	369	168	1970	3218	2.12	7.67
testfs1_tier2	1	0	2	0	0.00	0.00

# Using the locally saved configuration files

This chapter includes the following topics:

- [About configuring the locally saved configuration files](#)
- [Configuring the locally saved configuration files](#)
- [Using the option commands](#)
- [Modifying the maximum amount of memory used for instant rollback cache objects](#)
- [Modifying the amount of time an unused inode spends on a freelist](#)

## About configuring the locally saved configuration files

You can use the Veritas Access import and export features to save and restore configuration information. Saving configuration information is useful when you upgrade Veritas Access software and you want to backup and restore your configuration settings.

You can export the configuration settings and save them in a local file, or you can export configuration settings and save them to a remote machine as specified by a URL. You can import configuration settings from a local file, or you can import configuration settings from a remote machine as specified by a URL.

When you use the `System> config import local` or `System> config import remote` commands to import a locally saved configuration, you can import all configuration information in the file, or you can use the `config_type` option to control what type of configuration information is imported.

See [Table 19-1](#) for a list of configuration types you can import.

**Table 19-1** Import configuration types

Configuration type (config_type)	Description
network	Imports the DNS, LDAP, NIS, nsswitch settings (does not include IP).
admin	Imports a list of users and passwords. This list includes CIFS local users and groups.
all	Imports all configuration information.
report	Imports report settings.
system	Imports the NTP settings, timezone, and system options like <code>cfsmount_ontimeout</code> , <code>dmpio</code> , <code>dmptune</code> , <code>nfsd</code> , <code>ninodes</code> , <code>tunefstab</code> , and <code>vxtune</code> .
cluster_specific	Imports public IP addresses, virtual IP addresses, and console IP addresses. Be careful before using this import option. The network connection to the console server is lost after a configuration file is imported. You need to reconnect to the console server.
all_except_cluster_specific	Imports all configuration information except for cluster-specific information.
nfs	Imports the NFS settings.
cifs	Imports the CIFS settings. <b>Note:</b> To import cifs local users and groups you have to import the <code>admin</code> module also.
ftp	Imports the FTP setting.
backup	Imports the NBU client (excluding the virtual-name and the virtual-ip).
replication	Imports the replication settings.
storage_schedules	Imports the SmartTier information and automated snapshot schedules.
storage_quota	Imports the default quota values and the quota status information for file systems.
storage_fs_alert	Imports file system alert settings.

**Table 19-1** Import configuration types (*continued*)

Configuration type (config_type)	Description
storage_dedup	Imports file system deduplication settings.
compress_schedule	Imports the compression schedule.
defrag_schedules	Imports the defragmentation schedule.
smartio	Imports the SmartIO settings.

## Configuring the locally saved configuration files

### To list configuration settings

- ◆ To view locally saved configuration files, enter the following:

```
System> config list
```

### To export configuration settings either locally or remotely

- ◆ To export configuration settings locally, enter the following:

```
System> config export local file_name
```

For example:

```
System> config export local 2014_July_20
```

To export configuration settings remotely, enter the following:

```
System> config export remote URL
```

For example:

```
System> config export remote
```

```
ftp://admin@ftp.docserver.veritas.com/configs/config1.tar.gz
```

```
Password: *****
```

*file\_name* Specifies the saved configuration file.

*URL* Specifies the URL of the export file (supported protocols are FTP and SCP).

### To import configuration settings locally

- ◆ To import configuration settings locally, enter the following:

```
System> 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_quota}
```

*file\_name* Specifies the name of the configuration file to be imported saved in a local file.

*config\_type* Specifies the type of configuration to import.

This parameter is optional.

If *config\_type* is left blank, *config\_type* defaults to all.

See [“About configuring the locally saved configuration files”](#) on page 313.

For example:

```
System> config import local 2014_July_20 network  
Backup of current configuration was saved as 200907150515  
network configuration was imported  
Configuration files are replicated to all the nodes
```

where 200907150515 is the date (20090715 = July 15, 2014) and the time (0515 = hour 5 and 15 minutes).

### To import configuration settings remotely

- ◆ To import configuration settings remotely, enter the following:

```
System> 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_quota}
```

*file\_name* Specifies the saved configuration file.

*URL* Specifies the saved configuration at a remote machine as specified by a URL.

*config\_type* Specifies the type of configuration to import.

This parameter is optional.

If *config\_type* is left blank, *config\_type* defaults to *all*.

See [“About configuring the locally saved configuration files”](#) on page 313.

For example:

```
System> config import remote ftp://user1@server.com/home/user1/
2014_July_20.tar.gz report
Password: *****
```

### To delete the locally saved configuration file

- ◆ To delete the locally saved configuration file, enter the following:

```
System> config delete file_name
```

*file\_name* Specifies the locally saved configuration file for which to delete.

# Using the option commands

## To display or change the NFS daemons

- 1 To display the number of NFS daemons, enter the following:

```
System> option show nfsd
```

For example:

```
System> option show nfsd
NODENAME                NUMBER_DAEMONS
-----                -
access_01                96
access_02                96
```

- 2 To change the number of NFS daemons, enter the following:

```
System> option modify nfsd number [nodename]
```

The range for the number of daemons is from 1 to 512.

For example:

```
System> option modify nfsd 97
```

## To display or modify the CFSmount online timeout

- 1 To display the CFSmount online timeout, enter the following:

```
System> option show cfsmount_ontimeout
```

- 2 To modify the CFSmount online timeout, enter the following:

```
System> option modify cfsmount_ontimeout value
```

The range is from 300 to 9000.

The default value for the CFSmount online timeout is 1200 seconds.

**To display, change, or view the statistics of the DMP I/O policy**

- 1 To display the `dmpio` policy, enter the following:

```
System> option show dmpio
```

For example:

NODENAME	TYPE	ENCLR/ARRAY	IOPOLICY
-----	-----	-----	-----
access_01	arrayname	disk	balanced
access_01	enclosure	disk	minimumq

If you want to view your current `enclosure` names, use the following command:

```
Storage> disk list detail
```

For example:

```
Storage> disk list detail
```

Disk	Pool	Enclosure	Size
=====	=====	=====	=====
sda_01	p1	OTHER_DISKS	10.00G

ID	Serial Number
==	=====
VMware%2C:VMware%20Virtual%20S:0:0	-

2 To change the DMP I/O policy, enter the following:

```
System> option modify dmpio
{enclosure enclr_name|arrayname array_name|arraytype {A/A|A/P|...}}
  iopolicy={adaptive|adaptiveminq|balanced|minimumq|priority|
round-robin|singleactive}
```

The `dmpio` policy variables are the following:

<code>enclosure</code>	<i>enclr_name</i>	Name of the enclosure to distinguish between arrays having the same array name.
<code>arrayname</code>	<i>array_name</i>	Name of the array. Two physical array boxes of the same make have the same array name.
<code>arraytype</code>	<i>array_type</i>	A multi-pathing type of array. Use one of the following:  active-active, active-active-A, active-active-A-HDS, active-active-A-HP, APdisk, active-passive, active-passive-C, active-passiveF-VERITAS, active-passiveF-T3PLUS, active-passiveF-LSI, active-passiveG, active-passiveG-C, Disk, CLR-A-P, CLR-A-PF

<code>iopolicy</code>	<code>adaptive</code>	In storage area network (SAN) environments, this option determines the paths that have the least delays, and schedules the I/O on the paths that are expected to carry a higher load. Priorities are assigned to the paths in proportion to the delay.
	<code>adaptiveminq</code>	The 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.
	<code>balanced</code>	Takes into consideration the track cache to balance the I/O across paths.
	<code>minimumq</code>	Uses a minimum I/O queue policy. The I/O is sent on the 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 policy is the default for Active/Active (A/A) arrays.
	<code>priority</code>	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 performances, and you want to enforce load balancing manually.
	<code>round-robin</code>	Sets a standard round-robin policy for the I/O. This policy is the default for Active/Passive (A/P) and Asynchronous Active/Active (A/A-A) arrays.
	<code>singleactive</code>	The I/O is channeled through the single active path.

## To display or change the global inode cache size and the current number of incore inodes

- 1 To display the global inode cache size and the current number of incore inodes, enter the following:

```
System> option show ninodes
```

For example:

```
INODE_CACHE_SIZE  
-----  
600000
```

- 2 To change the global ninodes cache size, enter the following:

```
System> option modify ninodes number | Auto
```

*number*

Specifies the inode cache size that you want to change. The range for inode cache size is from 10000 to 8000000.

The maximum memory estimation can be calculated using the following guidelines:

- Each inode has a total of 4.75K size
- About 1.33k of size (3 inodes in 1 page)
- About 7 Global Lock Manager (GLM) locks with each GLM lock takes about 500 bytes

Example: 500k active incore inode

- 500k \* 4.75k = 2.38G

*Auto*

Indicates that the value for ninodes is automatically calculated based on memory size and other parameters.

When the *Auto* option is specified, the `System> option modify ninodes` command does not take any input. If *number* is specified, the `System> option modify ninodes` command hard-codes that value as the number of VxFS cached inodes. For any system memory (RAM), these number of inodes will always be in the system cache (once previously accessed by users).

In *Auto* mode, VxFS autotunes the value based on how much system memory (RAM) is available on that particular node. This helps control memory usage of cache, as selecting a random and large value of *number* can create memory pressures on Veritas Access.

For example:

```

System> option modify ninodes 1000000
INODE_CACHE_SIZE
=====
Auto
ACCESS System SUCCESS V-288-0 Successful to modify the cachesize to
1000000, but will need cluster wide reboot to reflect the tuning in
the kernel
Do you want to continue with cluster wide reboot (y/n)?
n
ACCESS System WARNING V-288-0 Cluster wide reboot not performed,
Please perform cluster reboot to reflect tuning in kernel
access_72>

```

## To display or modify the tunefstab parameter

- 1 To display the tunefstab parameter, enter the following:

```
System> option show tunefstab
```

For example:

```

System> option show tunefstab
NODENAME      ATTRIBUTE      VALUE
-----      -
access_01     write_throttle 0

```

- 2 To modify the tunefstab parameter, enter the following:

```
System> option modify tunefstab write_throttle value
```

where *value* is the number you assign to the write\_throttle parameter.

For example:

```

System> option modify tunefstab write_throttle 20003
System> option show tunefstab
NODENAME      ATTRIBUTE      VALUE
-----      -
access_01     write_throttle 20003
access_02     write_throttle 20003

```

## To display or modify the value of the dmptune attribute

- 1 To display the value of the `dmptune` attribute, enter the following:

```
System> option show dmptune
```

For example:

```
System> option show dmptune
NODENAME          ATTRIBUTE          VALUE
-----          -
access_01         dmp_path_age      57
access_01         dmp_health_time   44
```

- 2 To modify the value of the `dmp_path_age` and `dmp_health_time` attributes, enter the following:

```
System> option modify dmptune {dmp_path_age value | dmp_health_time
value}
```

`dmp_path_age 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.

`dmp_health_time value` 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 DMP does not re-enable the path for I/O until the `dmp_path_age` seconds have elapsed.

The default value of `dmp_health_time` is 60 seconds. A value of 0 prevents DMP from detecting intermittently failing paths.

For example:

```
System> option modify dmptune dmp_path_age 40
```

```
System> option modify dmptune dmp_health_time 50
```

# Modifying the maximum amount of memory used for instant rollback cache objects

The `volpagemod_max_memsz` attribute specifies the maximum amount of memory that is allocated for instant rollback cache objects. The allocated memory is exclusively dedicated to the cache objects and is not available for other processes or applications.

Veritas Access automatically tunes the value of `volpagemod_max_memsz`. The default value is 6144 kilobytes. You can change the value of `volpagemod_max_memsz`, although Veritas Access overrides the value if required. When instant rollback volumes are created, Veritas Access doubles the value of the `volpagemod_max_memsz` attribute if the cache requires more memory.

The required size for this tunable parameter depends on the region size and the number of volumes for which space-optimized instant snapshots are taken. You can use the following formula:

$$\text{size\_in\_KB} = 6 * (\text{total\_filesystem\_size\_in\_GB}) * (64 / \text{region\_size\_in\_KB})$$

The default region size for a large file system is 256 KB. For example, a single 1 TB volume requires around 1536 KB of paging memory. If there were 10 such volumes, 15360 KB of paging memory would be required.

## To modify the `volpagemod_max_memsz` parameter

- 1 To display the existing value, enter the following:

```
System> option show vxtune
```

For example:

```
System> option show vxtune
NODENAME      TUNABLE                VALUE (KB)
-----      -
access_01    volpagemod_max_memsz  6144
access_02    volpagemod_max_memsz  6144
```

- 2 To modify the `volpagemod_max_memsz` parameter, enter the following:

```
System> option modify vxtune volpagemod_max_memsz value
```

For example:

```
System> option modify vxtune volpagemod_max_memsz 15360
```

# Modifying the amount of time an unused inode spends on a freelist

In VxFS, an inode is put on a freelist if it is not used. The memory space for this unused inode can be freed if it stays on the freelist for `vx_timelag` number of seconds. The `vx_timelag` parameter lets you specify the minimum amount of time an unused inode spends on a freelist before its memory space is freed.

The default value for `vx_timelag` is 180 seconds.

Increasing the `vx_timelag` parameter improves read performance because the inode stays in memory for a longer time. Veritas recommends changing the `vx_timelag` parameter to a higher value to improve read performance.

Use the `vx_timelag` parameter for read-intensive workloads only, and only if the cluster has sufficient memory. Do not change the `vx_timelag` parameter if the workload is not write-intensive.

---

**Note:** The `vx_timelag` parameter is a system-wide tunable, and it affects all the file systems in the Veritas Access cluster.

---

## To modify the `vx_timelag` value

- ◆ Enter the following to change the value for `vx_timelag`:

```
System> option modify vxfs vx_timelag seconds
```

Where *seconds* represent the amount of time that an unused inode spends on a freelist.

For example:

```
System> option modify vxfs vx_timelag 3600
```

You need to perform a restart of your cluster for the change in the `vx_timelag` value to take effect.

### To display the existing vx\_timelag value

- ◆ Enter the following to display the existing value of vx\_timelag:

```
System> option show vxfs
```

For example:

```
System> option show vxfs
```

```
NODENAME      ATTRIBUTE    VALUE
=====      =====    =====
access_72_01  vx_timelag  10
```

```
System> option modify vxfs vx_timelag 600
```

```
ACCESS System INFO V-288-0 Successfully modified value vx_timelag
to 600 but will need cluster wide reboot to reflect the tuning in the
kernel
```

```
Do you want to continue with cluster wide reboot (y/n)?
```

# Veritas Access tuning

This chapter includes the following topics:

- [File system mount-time memory usage](#)

## File system mount-time memory usage

Mounting a file system on a computer system allocates system memory that is not freed until the file system is unmounted. The amount of memory allocated at mount time is directly proportional to the size of the file system being mounted. The amount of memory that is allocated at mount-time is therefore important information to help determine the system memory requirements for a Veritas Access environment. The mount-time memory requirement is different if you expect to mount a total of 1 PB of storage or 2 PBs of storage. The number of files currently in the file system does not affect the amount of memory allocated at mount-time. The amount of memory allocated at mount-time is also inversely proportional to the file system block size.

The information required to determine the amount of memory allocated at mount time is the total size of all the file systems that are mounted on the same computer system at the same time and the block size of each file system.

The amount of memory allocated at mount time can therefore be estimated by obtaining the total size of all the file systems that are mounted on a system according to the file system block size. So four totals in all, one for each file system block size of 1 KB, 2 KB, 4 KB, and 8 KB.

**Table 20-1** File system mount-time memory usage

File system block size	Total size of mounted file systems	Memory allocation at mount time
1 KB	'a' TBs	'w'MBs allocated per TB
2 KB	'b' TBs	'x'MBs allocated per TB

**Table 20-1** File system mount-time memory usage (*continued*)

File system block size	Total size of mounted file systems	Memory allocation at mount time
4 KB	'c' TBs	'y'MBs allocated per TB
8 KB	'd' TBs	'z'MBs allocated per TB

The mount-time memory requirement is therefore:

$$((a*w) + (b*x) + (c*y) + (d*z))$$

A file system using a 1 KB block size (the smallest file system block size) allocates approximately eight times more memory at mount time than a file system of the same size using a 8 KB block size (the largest file system block size). For this reason, the Veritas Access file system defaults to a block size of 8 KB if a block size is not specified when creating a file system.

Some customers might like to create small file systems using a 1 KB file system block size and subsequently grow the file system size significantly, as the file system block size cannot be changed after the file system is created. This procedure can result in very large file systems using a 1 KB block size that can result in an unexpectedly large allocation of system memory at mount time.

A Clustered File System (CFS) primary mount requires slightly more memory allocated at mount-time than a CFS secondary. The performance team recommends that the memory utilization of a CFS primary be used as the guideline for calculating the file system mount-time memory requirement.

**Table 20-2** Memory footprint of 16 file systems with 32 TB size each - CFS primary mount

		32 TB each file system			
Block size/file system	CFS primary mount				
	Memory used (MB)				
	1 KB	2 KB	4 KB	8 KB	
1	329	164	82	41	
2	659	328	165	82	
3	988	491	248	125	
4	1326	657	337	166	
5	1649	821	414	210	

**Table 20-2** Memory footprint of 16 file systems with 32 TB size each - CFS primary mount (*continued*)

	<b>32 TB each file system</b>			
6	1977	985	498	249
7	2306	1150	581	291
8	2635	1329	665	333
9	2964	1483	747	375
10	3293	1646	829	418
11	3624	1810	913	459
12	3953	1975	995	534
13	4281	2140	1077	546
14	4614	2307	1161	589
15	4942	2471	1243	629
16	5272	2636	1325	671

**Table 20-3** Memory footprint of 16 file systems with 32 TB size each - CFS secondary mount

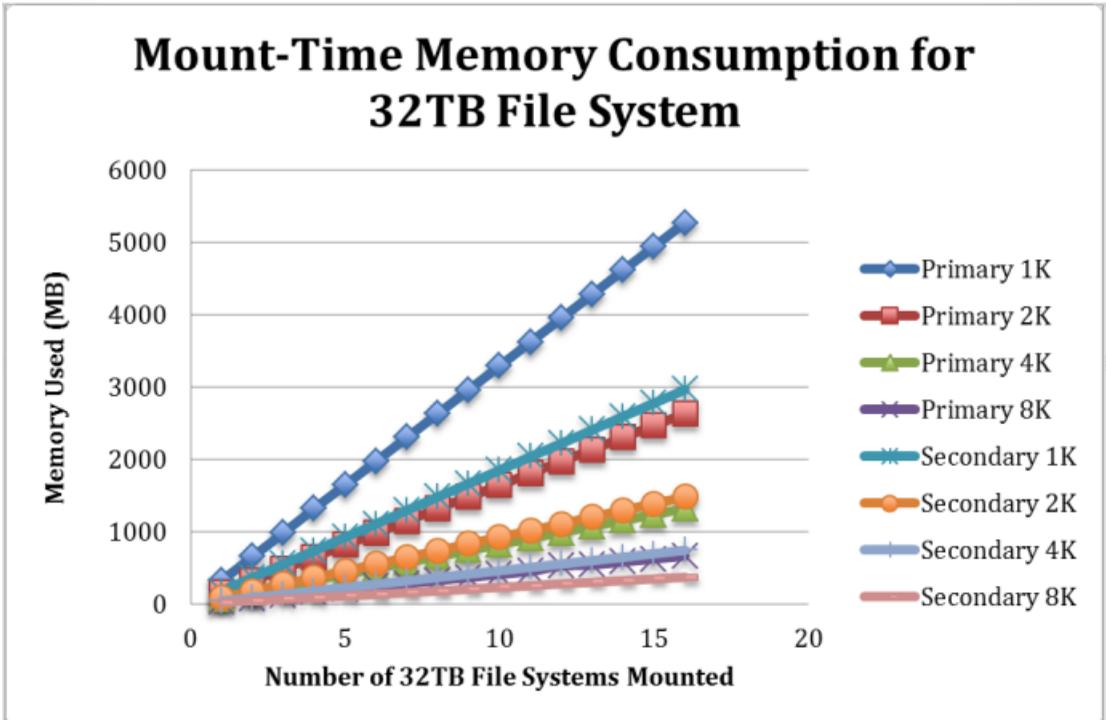
	<b>32 TB each file system</b>			
Block size/file system	CFS secondary mount			
	Memory used (MB)			
	1 KB	2 KB	4 KB	8 KB
1	187	93	47	21
2	372	186	94	48
3	558	279	139	71
4	742	371	186	94
5	929	465	233	117
6	1113	557	280	140
7	1300	650	326	164

**Table 20-3** Memory footprint of 16 file systems with 32 TB size each - CFS secondary mount (*continued*)

	32 TB each file system			
8	1485	743	373	187
9	1670	837	419	213
10	1854	928	465	237
11	2040	1020	512	259
12	2224	1114	558	286
13	2410	1208	606	306
14	2596	1301	652	330
15	2780	1393	701	353
16	2966	1485	747	376

[Figure 20-1](#) provides the guideline for the system memory utilization at mount time.

Figure 20-1 Mount-time memory consumption for 32 TB file systems



# Provisioning and managing shares

- [Chapter 21. Creating and maintaining file systems](#)
- [Chapter 22. Creating shares for applications](#)
- [Chapter 23. Creating and maintaining NFS shares](#)
- [Chapter 24. Creating and maintaining CIFS shares](#)
- [Chapter 25. Creating and maintaining S3 shares](#)

# Creating and maintaining file systems

This chapter includes the following topics:

- [About creating and maintaining file systems](#)
- [About scale-out file systems](#)
- [Considerations for creating a file system](#)
- [Creating a file system](#)
- [Bringing the file system online or offline](#)
- [Listing all file systems and associated information](#)
- [Modifying a file system](#)
- [About quotas for usage](#)
- [Managing a file system](#)
- [Destroying a file system](#)
- [Upgrading disk layout versions](#)

## About creating and maintaining file systems

A Veritas Access environment consists of multiple nodes that can access and update files in the same Veritas file system at the same time. Many file systems can be supported at the same time. You create file systems on groups of disks called storage pools.

File systems consist of both metadata and file system data. Metadata contains information such as the last modification date, creation time, permissions, and so on. The total amount of the space that is required for the metadata depends on the number of files in the file system. A file system with many small files requires more space to store metadata. A file system with fewer larger files requires less space for handling the metadata.

When you create a file system, you need to set aside some space for handling the metadata. The space that is required is generally proportional to the size of the file system. For this reason, after you create the file system, a small portion of the space appears to be used. The space that is set aside to handle metadata may increase or decrease as needed. For example, a file system on a 1 GB volume takes approximately 35 MB (about 3%) initially to store metadata. In contrast, a file system of 10 MB requires approximately 3.3 MB (30%) initially for storing the metadata.

File systems can be increased or decreased in size. SmartTier functionality is also provided at the file system level.

See [“About Veritas Access SmartTier”](#) on page 476.

Any file system can be enabled for deduplication.

## About scale-out file systems

Veritas Access provides a scale-out file system that manages a single namespace spanning over on-premises storage and cloud storage, which provides better fault tolerance for large data sets. Currently a scale-out file system can hold up to 266 TB. 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 file system is exported.

You can find what virtual IP address is associated with a scale-out file system by using the `NFS> share show` command.

Veritas Access only supports access to scale-out file systems using NFS-Ganesha. NFS shares that are created on scale-out file systems must be mounted on the NFS clients using the virtual IP address that is associated with the NFS share.

See [“Using the NFS-Ganesha server”](#) on page 142.

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 (Amazon S3) can be one of the storage containers. One of the storage containers stores the metadata and the other containers store the actual data. This data can be on-premises or can be in Amazon S3. 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.

See [“Characteristics of a scale-out file system”](#) on page 336.

You can configure Amazon S3 as a cloud container. Amazon S3 is the only supported cloud provider. Data can be moved between the on-premises container and the cloud container.

See [“Configuring the cloud as a tier feature for scale-out file systems”](#) on page 497.

See [“Moving files between tiers in a scale-out file system”](#) on page 498.

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.
- You can resize (grow) a scale-out file system up to 266 TB.
- The minimum size of a scale-out file system is 10 GB.

## Characteristics of a scale-out file system

With a scale-out file system, you can move data to the Amazon S3 cloud using a tiering mechanism. The cloud as tier feature is best used for moving infrequently accessed data to the cloud.

---

**Note:** Do not attempt transactional workloads on the files that have been moved to the cloud.

---

See [“Configuring the cloud as a tier feature for scale-out file systems”](#) on page 497.

The following operations are supported for scale-out file systems:

- Active/Passive access
- Grow or shrink the size of a scale-out file system
- NFS protocol support

The following operations are not supported for scale-out file systems:

- Write operations and truncation of files are not supported for the files that are stored on the cloud tier. If you want to modify the files on the cloud tier, bring the files on-premises first.
- You cannot use the CIFS and S3 protocols with a scale-out file system.
- Not all of the storage commands are supported for scale-out file systems.

# Considerations for creating a file system

The following sections describe the considerations and best practices for creating file systems.

## Best practices for creating file systems

The following are the best practices for creating file systems:

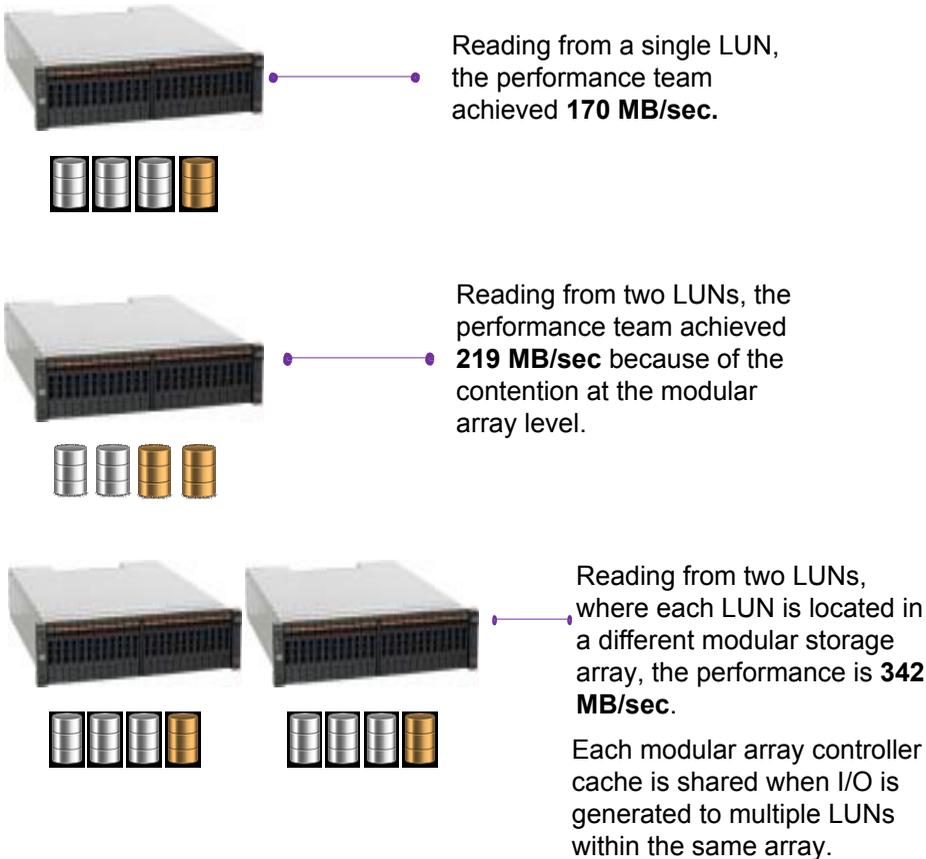
- Ensure all the disks (LUNs) in each storage pool have an identical hardware configuration.  
 Best performance results from a striped file system that spans similar disks. The more closely you match the disks by speed, capacity, and interface type, the better the performance you can expect. When striping across several disks of varying speeds, performance is no faster than that of the slowest disk.
- Create striped file systems rather than simple file systems when creating your file systems.  
 See [“About striping file systems”](#) on page 340.
- In a given storage pool, create all the file systems with the same number of columns.
- Ensure that the number of disks in each storage pool is an exact multiple of the number of columns used by the file systems created in that storage pool.
- Consider how many disks you need to add to your storage pool to grow your striped file systems.  
 A 5-TB file system using five columns cannot be grown in a storage pool containing 8\*1-TB disks, despite having 3 TB of disk space available. Instead create the file system with either four or eight columns, or else add 2\*1-TB disks to the pool. See further examples in the table.

Use case	Action	Result
storage pool with eight disks of the same size (1 TB each)	Create a 5 TB striped file system with five columns.	You cannot grow the file system greater than 5 TB, even though there are three unused disks.
storage pool with eight disks of the same size (1 TB each)	Create a 5 TB striped file system with eight columns.	You can grow the file system to 8 TB.

storage pool with eight disks of the same size (1 TB each)	Create a 4 TB striped file system with four columns.	You can grow the file system to 8 TB.
storage pool with eight disks of the same size (1 TB each)	Create a 3 TB striped file system with three columns.	You cannot grow the file system to 8 TB.
storage pool with eight disks of the different sizes (3 are 500 GB each, and 5 are 2 TB each)	Create an 8 TB striped file system with eight columns.	You cannot create this 8-TB file system.

- Consider the I/O bandwidth requirement when determining how many columns you require in your striped file system.  
Based on the disks you have chosen, I/O throughput is limited and potentially restricted. [Figure 21-1](#) describes the LUN throughput restrictions.
- Consider populating each storage pool with the same number of disks from each HBA. Alternatively, consider how much of the total I/O bandwidth that the disks in the storage pool can use.  
If you have more than one card or bus to which you can connect disks, distribute the disks as evenly as possible among them. That is, each card or bus must have the same number of disks attached to it. You can achieve the best I/O performance when you use more than one card or bus and interleave the stripes across them.
- Use a stripe unit size larger than 64 KB. Performance tests show 512 KB as the optimal size for sequential I/O, which is the default value for the stripe unit. A greater stripe unit is unlikely to provide any additional benefit.
- Do not change the operating system default maximum I/O size of 512 KB.

**Figure 21-1** LUN throughput - details on the LUN throughput restrictions



## Choosing a file system layout type

Veritas Access allows you to create file systems with several layout types. [Table 21-1](#) describes the layout types and the advantages of each.

**Table 21-1** Types of volume layout

Layout type	Description
Simple	Arranges the disks sequentially and contiguously. A simple layout allows a file system to be created from multiple regions of one or more disks if there is not enough space on a single region of a disk.

**Table 21-1** Types of volume layout (*continued*)

Layout type	Description
Striped	Spreads the data evenly across multiple disks. Stripes are equal-sized fragments that are allocated alternately and evenly to the disks. Throughput increases with the number of disks across which a file system is striped. Striping helps to balance I/O load in cases where high traffic areas exist on certain disks.
Mirrored	Mirrors the information contained in the file system to provide redundancy of data. For the redundancy to be useful, each mirror should contain disk space from different disks.
Mirrored-stripe	Configures a striped file system and then mirrors it. This requires at least two disks for striping and one or more other disks for mirroring (depending on whether the mirror is simple or striped). The advantages of this layout are increased performance by spreading data across multiple disks and redundancy of data.
Striped-mirror	Configures several mirrors as the columns of a striped file system. This layout offers the same benefits as a mirrored-stripe file system. In addition, it provides faster recovery as the failure of single disk does not force an entire striped mirror offline.

## About striping file systems

You can obtain huge performance benefits by striping (RAID-0) using software-defined storage (SDS). You achieve performance benefits regardless of the choice of LUN configuration in your storage hardware. Striping is useful if you need large amounts of data that is written to or read from physical disks, and consistent performance is important. SDS striping is a good practice for all Veritas Access use cases and workloads.

Veritas strongly recommends that you create striped file systems when creating your file system for the following reasons:

- Maximize the I/O performance.
- Proportion the I/O bandwidth available from the storage layer.
- Balance the I/O load evenly across multi-user applications running on multiple nodes in the cluster.

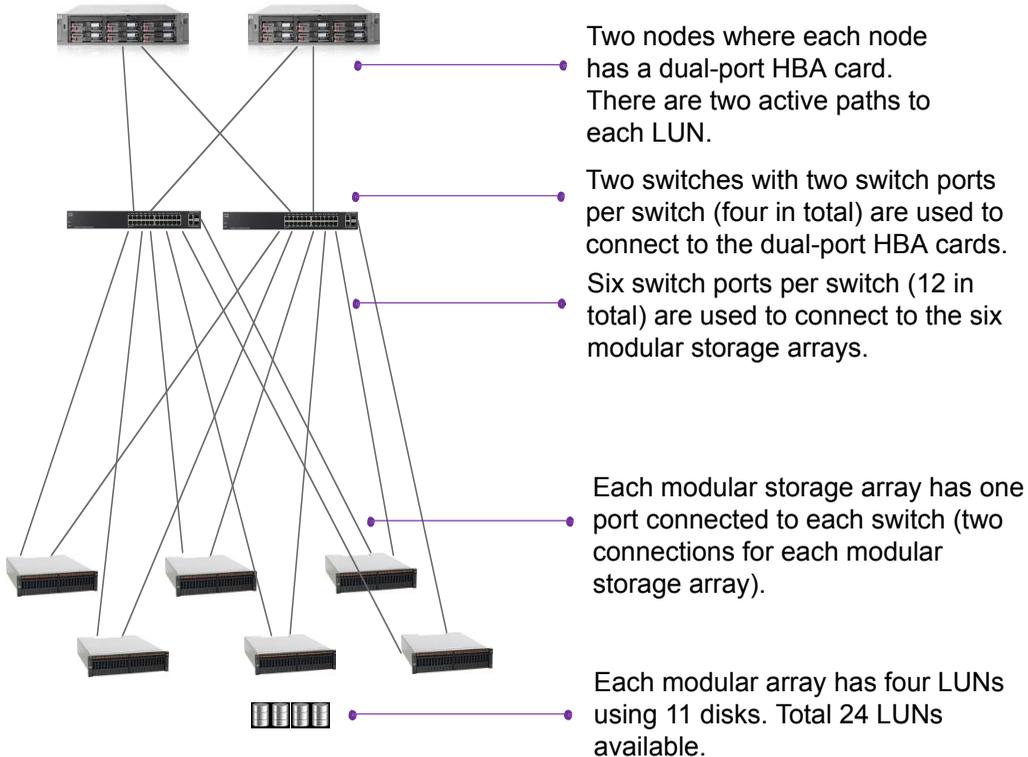
However there are also pitfalls to avoid.

The following information is essential before selecting the disks to include in your striped file system:

- Understanding of your hardware environment

- Storage capabilities and limitations (bottlenecks)
- Choice of LUNs (each LUN, or disk, equates to a column in a SDS-striped volume)

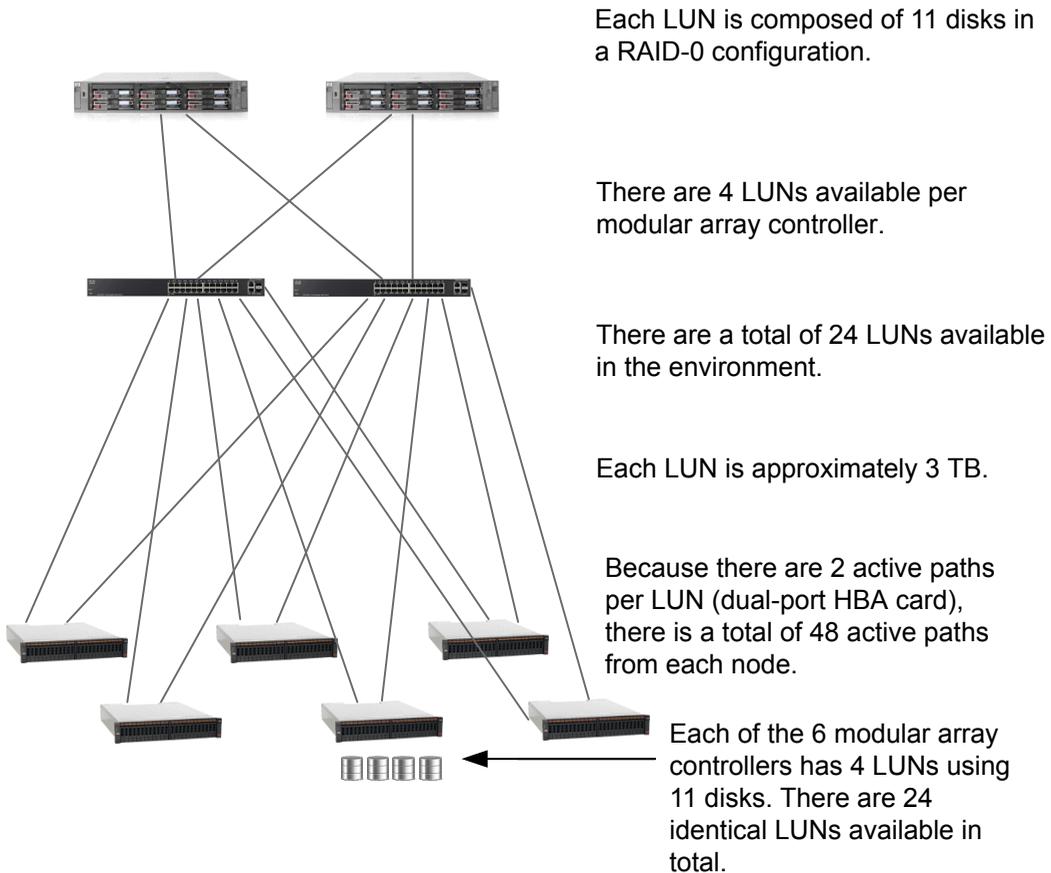
**Figure 21-2** An example hardware configuration



An extreme example might be if one column (equal to one LUN) is composed of only hard disk drives (HDDs) in the storage array. All of the other columns in the same striped volume are composed of only SSDs in the storage array. The overall I/O performance bottlenecks on the single slower HDD LUN.

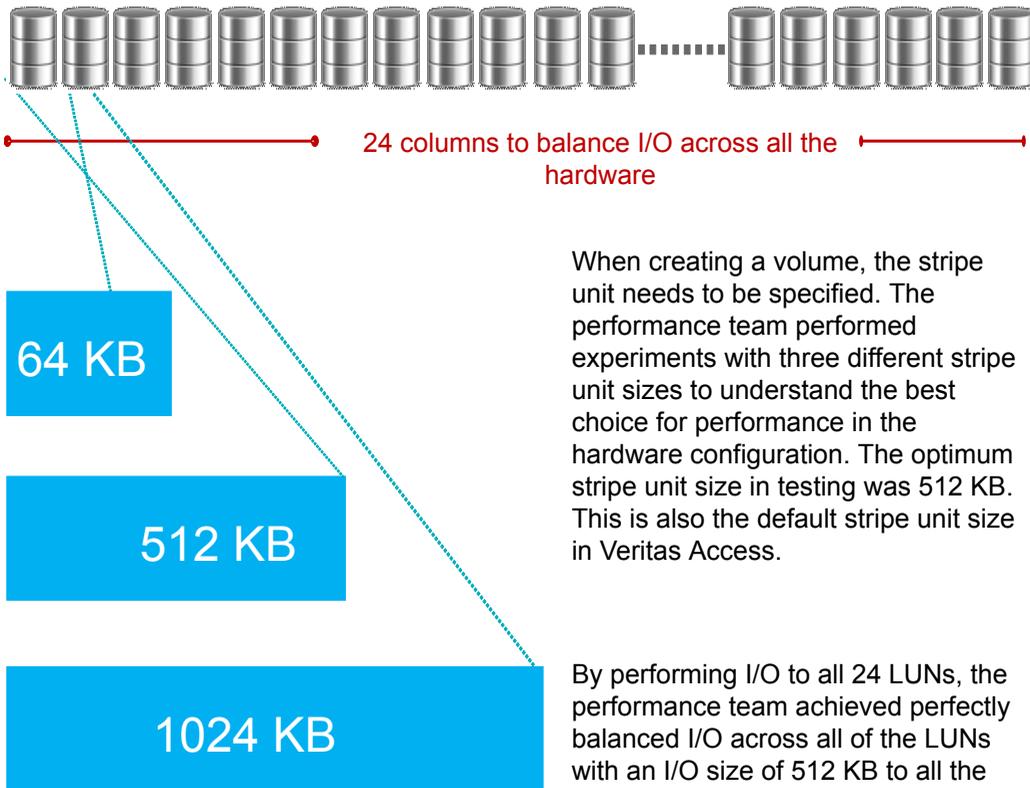
Understanding the LUN configuration and ensuring that all of the LUNs have an identical configuration is therefore essential for maximizing performance and achieving balanced I/O across all the LUNs.

**Figure 21-3** LUN configuration



All 24 LUNs have an identical hardware configuration.

**Figure 21-4** Volume configuration



When creating a volume, the stripe unit needs to be specified. The performance team performed experiments with three different stripe unit sizes to understand the best choice for performance in the hardware configuration. The optimum stripe unit size in testing was 512 KB. This is also the default stripe unit size in Veritas Access.

By performing I/O to all 24 LUNs, the performance team achieved perfectly balanced I/O across all of the LUNs with an I/O size of 512 KB to all the path devices.

The performance team created a volume with 24 columns to use the entire storage bandwidth in one file system. Veritas does not advise changing the operating system default maximum I/O size of 512 KB. The optimum stripe-unit size is 512 KB.

## Determining the initial extent size for a file system

Veritas File System (VxFS) determines the size of the first extent that is allocated based on the first write to a new file. Normally, the first extent is the smallest power of 2 that is larger than the size of the first write. If that power of 2 is less than 8 KB (the default file system block size), the first extent that is allocated is 8 KB. After the initial extent is allocated, the file system increases the size of subsequent extents with each allocation as the file size is increased using extending writes.

The initial extent size is tunable, and can be changed using the `System> option modify tunefstab` command.

Increasing the initial extent size to a larger value helps to reduce file system fragmentation and improves I/O performance.

The best value for the initial extent size depends on the expected file sizes that are created by the application. The maximum value is 32768, which equates to a 256 MB extent allocation using the default 8 KB file system block size. Any over allocation of space is returned to the free space pool after the file is closed.

If the application creates a lot of small files with an exact size of 1 MB, then the initial extent size can be set to 128 (1 MB). If 1 MB is an approximate file size, then the initial extent size can be set to 64 (512 KB) instead. If most files are approximately 1 GB or greater in size, then the maximum value of 32768 can be used.

## About creating a tuned file system for a specific workload

Veritas Access provides an easy way to create a well-tuned file system for a given type of workload.

You can use the newly created file system for the following common client applications:

- Virtual machine workloads
- Media server workloads  
Streaming media represents a new wave of rich Internet content. Recent advancements in video creation, compression, caching, streaming, and other content delivery technology have brought audio and video together to the Internet as rich media. You can use Veritas Access to store your rich media, videos, movies, audio, music, and picture files.

See the `Storage> fs man` page for more information.

```
Storage> fs create pretuned media_fs 100g pool2 workload=mediaserver layout=striped 8
```

The `workload=mediaserver` option creates a file system called `media_fs` that is 100g in size in `pool2` striped across eight disks.

---

**Note:** You can select only one workload for a specified file system. You specify the workload when you create the file system, and you cannot change the workload after you have created the file system.

---

### Virtual machine workloads

A virtual machine disk file, also known as a VMDK file, is a file held in the Veritas Access file system that represents a virtual disk for a virtual machine. A VMDK file is the same size as the virtual disk, so VMDK file sizes are typically very large. As

writes are performed to the virtual disk within the virtual machine, the VMDK file is populated with extents in the Veritas Access file system. Because the VMDK files are large, they can become heavily fragmented, which gradually impedes performance when reading and writing to the virtual disk. If you create a file system specific to a virtual machine workload, Veritas Access internally tunes the file system to allocate a fixed extent size of 1MB for VMDK files. The 1MB block size significantly reduces both file system and VMDK file fragmentation while improving the virtual machine workload performance.

## Media server workloads and tunable for setting write\_throttle

Media server workloads involve heavy sequential reads and writes. Striping across multiple disks yields better I/O latency.

See [“Best practices for creating file systems”](#) on page 337.

For media server workloads, Veritas Access provides a tunable that can help restrict the amount of write I/O throughput. The tunable helps prevent the streaming of information (sequential reads) from being affected by other processes performing write I/O on the same NAS server. An example use case is as follows. You want to stream a movie, this is reading a file (sequential reads). You do not want the movie experience to pause due to buffering. Another user might be uploading new content to the same file system (the upload is writing data to a different file). The uploading (writing) can cause the streaming (reading) to pause due to buffering. Veritas Access throttles the writing processes so that they do not consume too much of the system memory.

Each file system must tune the value `write_throttle` independently of other file systems. The default value is 0, which implies there is no `write_throttle`. The throttle is per file, so when writing to multiple files at the same time, the `write_throttle` threshold applies to each file independently.

Setting a non-zero value for a file system prevents the number of dirty memory pages that are associated with the file from increasing beyond the threshold. If you set a `write_throttle` value of 256, then writes to a file pause to flush the file to disk once 256 dirty memory pages have built up for the file. After the number of dirty pages for a file reaches the `write_throttle` threshold, further dirtying of pages is paused, and the file system starts flushing the file's pages to disk, even if free memory is available. Each memory page is 4KB of file data, so 256 pages is 1MB of file data. Setting a value for `write_throttle` means a writing thread pauses upon reaching the threshold (on the NAS server) while the file's dirty pages are flushed to disk, before resuming further writes to that file. Once flushed, the dirty pages become clean pages, which means the memory (the pages) can then be reused for perhaps pre-fetching data from disk for streaming reads. Setting a value for

`write_throttle` helps prevent write I/O from consuming too much of the system memory.

Setting `write_throttle` requires some experimentation, which is why Veritas Access does not set a non-zero value by default. The valid range for `write_throttle` is 0 to 2048 pages. A good starting value for experimentation is 256.

## About FastResync

The FastResync feature performs quick and efficient resynchronization of stale mirrors (a mirror that is not synchronized). FastResync optimizes mirror resynchronization by keeping track of updates to stored data that have been missed by a mirror.

When FastResync has been enabled, it does not alter how you administer mirrors. The only visible effect is that repair operations conclude more quickly.

## Creating a file system

Veritas Access supports the following types of file systems:

- Cluster File System (CFS) - creates a standard CFS file system. The CFS file system is the default file system when creating a new file system.
- scale-out - creates a scale-out file system that manages a single namespace spanning over both on-premises storage as well as cloud storage. See [“About scale-out file systems”](#) on page 335.

Veritas Access supports the following file system layouts:

- Simple - creates a file system of a specified size, and you can specify a block size for the file system.
- Mirrored - creates a mirrored file system with a specified number of mirrors along with a list of pools and online status.
- Mirrored-stripe - creates a mirrored-stripe file system with a specified number of columns, mirrors, pools, and protection options.
- Striped - creates a striped file system. A striped file system is a file system that stores its data across multiple disks rather than storing the data on just one disk.
- Striped-mirrored - creates a striped-mirror file system with a specified number of columns, mirrors, pools, and protection options.

The default block size is determined based on the size of the file system when the file system is created. For example, 1 KB is the default block size for up to a 2-TB file system size. Other default block sizes, 2 KB, 4 KB, and 8 KB are available for

different ranges of file system sizes. If you create a 1-TB file system, and then increase it to 3 TB, the file system block size remains at 1 KB.

See the `storage_fs(1)` man page for detailed examples.

You can also create a file system for customized workloads.

See [“About creating a tuned file system for a specific workload”](#) on page 344.

---

**Note:** If the configuration file system creation fails, the originating file system request also fails. Veritas Access requires at least two disks for the mirrored configuration file system, and in case of Flexible Shared Storage (FSS), at least two nodes are required to be part of the storage pool.

---

### To create a simple file system of a specified size

- ◆ Create a simple file system with a specified size.

```
Storage> fs create simple fs_name size
      pool1[,disk1,...] [blksize=bytes]
```

For example:

```
Storage> fs create simple fs2 10m sda
100% [#] Creating simple filesystem
```

### To create a mirrored file system

- ◆ Create a mirrored file system.

```
Storage> fs create mirrored fs_name size nmirrors
      pool1[,disk1,...] [protection=disk|pool] [blksize=bytes]
```

For example:

```
Storage> fs create mirrored fs1 100M 2 pool1,pool2
100% [#] Creating mirrored filesystem
```

### To create a mirrored-stripe file system

- ◆ Create a mirrored-stripe file system.

```
Storage> fs create mirrored-stripe fs_name size nmirrors
      ncolumns pool1[,disk1,...]
      [protection=disk|pool] [stripeunit=kilobytes] [blksize=bytes]
```

### To create a striped-mirror file system

- ◆ Create a striped-mirror file system.

```
Storage> fs create striped-mirror fs_name size nmirrors
ncolumns pool1[,disk1,...]
[protection=disk|pool] [stripeunit=kilobytes] [blksize=bytes]
```

### To create a striped file system

- ◆ Create a striped file system.

```
Storage> fs create striped fs_name size ncolumns
pool1[,disk1,...] [stripeunit=kilobytes]
[blksize=bytes]
```

### To create a simple scale-out file system

- ◆ Create a simple scale-out file system.

```
Storage> fs create largefs simple fs_name size
pool1 [blksize=bytes]
```

You can create the same types of file system layouts for a scale-out file system as for a Cluster File System (CFS) file system.

Example:

```
Storage> fs create largefs simple scfs1 100G pool1
```

<code>fs_name</code>	Specifies the name of the file system being created. The file system name should be a string. If you enter a file that already exists, you receive an error message and the file system is not created.
<code>size</code>	<p>Specifies the size of a file system.</p> <p>To create a file system, you need at least 10 MB of space.</p> <p>You can create a file system in the following units:</p> <ul style="list-style-type: none"> <li>■ MB</li> <li>■ GB</li> <li>■ TB</li> </ul> <p>You can enter the units with either uppercase (10 M) or lowercase (10 m) letters.</p> <p>To see how much space is available on a pool, use the <code>Storage&gt; pool free</code> command.</p>

nmirrors	<p>Specifies the number of mirrors for the file system. You must enter a positive integer.</p>
ncolumns	<p>Specifies the number of columns for the striped file system. The number of columns represents the number of disks to stripe the information across. If the number of columns exceeds the number of disks for the entered pools, an error message is displayed. This message indicates that there is not enough space to create the striped file system.</p>
pool1[,disk1,...]	<p>Specifies the pool(s) or disk(s) for the file system. If you specify a pool or disk that does not exist, you receive an error message. You can specify more than one pool or disk by separating the name with a comma. Do not include a space between the comma and the name.</p> <p>To find a list of pools and disks, use the <code>Storage&gt; pool list</code> command. To find a list of disks, use the <code>Storage&gt; disk list</code> command.</p> <p>The disk must be part of the pool or an error message is displayed.</p>
protection	<p>If you do not specify a protection option, the default is "disk."</p> <p>The available options for this field are:</p> <ul style="list-style-type: none"> <li>■ disk - Creates mirrors on separate disks.</li> <li>■ pool - Creates mirrors in separate pools. If there is not enough space to create the mirrors, an error message is displayed, and the file system is not created.</li> </ul> <p>The <code>protection=pool</code> option is not supported for an isolated pool.</p>
stripeunit=kilobytes	<p>Specifies a stripe unit (in kilobytes).</p> <p>The following are the possible values:</p> <ul style="list-style-type: none"> <li>■ 128</li> <li>■ 256</li> <li>■ 512 (default)</li> <li>■ 1024</li> <li>■ 2048</li> </ul>

blksize=bytes

Specifies the block size for the file system.

The following are the possible values in bytes:

- 1024
- 2048
- 4096
- 8192 (default)

Block sizes can affect the file size. For example, to create a file system greater than 32 TB, the block size needs to be 8192.

pdir\_enable

Specifies if you want to enable a partition directory for the file system. By default, this feature is not enabled.

After a file system is created, the file system reserves some space for internal logging. Internal logging provides additional data integrity. Due to the space that is reserved for internal logging, the file system may appear to be used immediately after file system creation. The space that is reserved for internal logging increases with the number of nodes in the Veritas Access cluster.

Log file sizes for the file systems are as follows:

10 GB to 100 GB    Log size = 60 MB per node

100 GB to 1 TB    Log size = 100 MB per node

1 TB and above    Log size = 256 MB per node

## Bringing the file system online or offline

The `Storage> fs online` or `Storage> fs offline` command lets you mount (online) or unmount (offline) a file system. You cannot access an offline file system from a client.

**To change the status of a file system**

- ◆ To change the status of a file system, enter one of the following, depending on which status you use:

```
Storage> fs online fs_name
Storage> fs offline fs_name
```

where *fs\_name* specifies the name of the file system that you want to mount (online) or unmount (offline). If you specify a file system that does not exist, an error message is displayed.

For example, to bring a file system online:

```
Storage> fs list
FS   STATUS   SIZE   LAYOUT  MIRRORS  COLUMNS  USE%
===  =====  ====  =====  =====  =====  =====
fs1  online   5.00G  simple  -         -         10%
fs2  offline  10.00M simple  -         -         -
```

```
NFS     CIFS     FTP     SECONDARY
SHARED  SHARED  SHARED  TIER
=====  =====  =====  =====
no      no      no      no
no      no      no      no
```

```
Storage> fs online fs2
100% [#] Online filesystem
```

```
Storage> fs list
FS   STATUS   SIZE   LAYOUT  MIRRORS  COLUMNS  USE%
===  =====  ====  =====  =====  =====  =====
fs1  online   5.00G  simple  -         -         10%
fs2  online   10.00M simple  -         -         100%
```

```
NFS     CIFS     FTP     SECONDARY
SHARED  SHARED  SHARED  TIER
=====  =====  =====  =====
no      no      no      no
no      no      no      no
```

For example, to place a file system offline:

```
Storage> fs offline fs1
100% [#] Offline filesystem
```

# Listing all file systems and associated information

## To list all file systems and associated information

- ◆ To list all file systems and associated information, enter the following:

```
Storage> fs list [fs_name]
```

where *fs\_name* is optional.

If you do not enter a specified file system, a list of file systems is displayed.

For example:

```
Storage> fs list fs1
General Info:
=====
Block Size:      8192 Bytes
Version:         Version 10
Cluster5_01:    online

Primary Tier
=====
Size:            40.00G
Use%:           0%
Layout:         mirrored-stripe
Mirrors:        2
Columns:        2
Stripe Unit:    512 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

Secondary Tier
=====
Size:            40.00G
Use%:           0%
Layout:         mirrored-stripe
Mirrors:        2
Columns:        2
```

```
Stripe Unit:      512 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

Defrag Status: Not Running
Fullfsck Status: Not Running
Resync Status:
  Tier 1, Mirror 02: 1.56% Start_time: Jun/20/2011/21:20:02 Work_time: 0:4:18
Remaining_time: 4:30:54
  Tier 2, Mirror 02: 0.21% Start_time: Jun/20/2011/21:33:20 Work_time: 0:0:4
Remaining_time: 32:03
Rollsync Status:
  Rollback alltask_roll, Tier 1: 0.16% Start_time: Jun/20/2011/19:12:45 Work_time: 0:0:3
Remaining_time: 30:29
  Rollback alltask_roll, Tier 2: 0.29% Start_time: Jun/20/2011/19:12:45 Work_time: 0:0:3
Remaining_time: 17:01
Relayout Status: Not Running
```

## Modifying a file system

You can modify a file system in the following ways:

- See [“Adding or removing a mirror from a file system”](#) on page 353.
- See [“Adding or removing a column from a file system”](#) on page 355.
- See [“Increasing the size of a file system”](#) on page 356.
- See [“Decreasing the size of a file system”](#) on page 358.

### Adding or removing a mirror from a file system

A mirrored file system is one that has copies of itself on other disks or pools.

#### To add a mirror to a file system

- ◆ To add a mirror to a file system, enter the following:

```
Storage> fs addmirror fs_name pool1[,disk1,...]
[protection=disk|pool]
```

- |                          |   |
|--------------------------|---|
| <b>fs_name</b>           | Specifies which file system to add the mirror. If the specified file system does not exist, an error message is displayed.  |
| <b>pool1[,disk1,...]</b> | <p>Specifies the pool(s) or disk(s) to use for the file system. If the specified pool or disk does not exist, an error message is displayed, and the file system is not created. You can specify more than one pool or disk by separating the name with a comma, but do not include a space between the comma and the name.</p> <p>To find a list of existing pools and disks, use the <code>Storage&gt; pool list</code> command.</p> <p>To find a list of the existing disks, use the <code>Storage&gt; disk list</code> command.</p> <p>The disk needs to be part of the pool or an error message is displayed.</p>  |
| <b>protection</b>        | <p>The default value for the protection field is <code>disk</code>.</p> <p>Available options are:</p> <ul style="list-style-type: none"> <li>■ <code>disk</code> - if the protection is set to <code>disk</code>, then mirrors are created on separate disks. This flag only works for file systems of type mirrored, mirrored-striped, and striped-mirror. The disks may or may not be in the same pool.</li> <li>■ <code>pool</code> - if the protection is set to <code>pool</code>, then mirrors are created in separate pools. This flag only works for file systems of type mirrored, mirrored-striped, and striped-mirror. If not enough space is available, then the file system creation operation fails.</li> </ul> |

For example:

```
Storage> fs addmirror fs1 pool3,pool4
```

### To remove a mirror from a file system

- ◆ To remove a mirror from a file system, enter the following:

```
Storage> fs rmmirror fs_name [pool_or_disk_name]
```

**fs\_name** Specifies the file system from which to remove the mirror. If you specify a file system that does not exist, an error message is displayed.

**pool\_or\_disk\_name** Specifies the pool or the disk name to remove from the mirrored file system that spans the specified pools or disks. If a pool name is the same as the disk name, then the mirror present on the pool is deleted.

For a striped-mirror file system, if any of the disks are bad, the `Storage> fs rmmirror` command disables the mirrors on the disks that have failed. If no disks have failed, Veritas Access chooses a mirror to remove.

For example:

```
Storage> fs rmmirror fs1 AMS_WMS0_0
```

## Adding or removing a column from a file system

You may want to add or remove a column from a file system in specific situations. Adding columns can help to perform more I/Os in parallel, so you may want to increase the number of columns in the file system.

---

**Note:** For a striped file system when you add a column, the layout that is displayed when you issue the `Storage> fs list` and `Storage> fs list fsname` commands may be different than the original layout of the file system while the layout (addition of new columns) operation is in progress. The original file system layout is displayed when the layout operation is completed.

---

**Note:** Adding and removing a column to and from a file system involves a volume-level layout. This is an I/O intensive operation. For a large file system, adding or removing columns takes a long time and can hurt application performance during this layout period.

---

### To add a specified number of columns to a file system

- ◆ To add a specified number of columns to a file system, enter the following:

```
Storage> fs addcolumn fs_name ncolumns pool_or_disk_name
```

**fs\_name** Specifies the file system for which you want to add additional columns.

**ncolumns** Specifies the number of columns that you want to add to the file system.

**Note:** In the case of a striped file system, the number of the disks that are specified should be equal to the number of columns (*ncolumns*).

**Note:** In the case of a mirrored-stripe and a striped-mirrored file system, the disks should be equal to (*ncolumns \* number\_of\_mirrors\_in\_fs*).

**pool\_or\_disk\_name** Specifies the pool or the disk name for the file system.

For example, to add two columns to file system fs1, enter the following:

```
Storage> fs addcolumn fs1 2 pool3
```

### To remove a column from a file system

- ◆ To remove a column from a file system, enter the following:

```
Storage> fs rmcolumn fs_name
```

where *fs\_name* is the name of the file system for which you want to remove the column.

For example:

```
Storage> fs rmcolumn fs1
```

## Increasing the size of a file system

To increase (grow) the size of a file system, it must be online. If the file system is not online, an error message is displayed, and no action is taken.

---

**Note:** For a scale-out file system, you can increase the size of the primary tier only.

---

See [“About scale-out file systems”](#) on page 335.

**To increase the size of a file system to a specified size**

- ◆ To increase the size of a file system to a specified size, enter the following:

```
Storage> fs growto {primary|secondary} fs_name new_length  
[pool[,disk1,...]]  
[protection=disk|pool]
```

For example:

```
Storage> fs growto primary fs1 1G
```

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 the `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.

**To increase the size of a file system by a specified size**

- ◆ To increase the size of a file system by a specified size, enter the following:

```
Storage> fs growby {primary|secondary} fs_name length_change  
[pool[,disk1,...]]  
[protection=disk|pool]
```

For example:

```
Storage> fs growby primary fs1 50M
```

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 the `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.

`primary|secondary` Specifies the primary or the secondary tier.

`fs_name` Specifies the file system whose size is increased. If you specify a file system that does not exist, an error message is displayed.

new_length	<p>Expands the file system to a specified size. The size that you specify must be a positive number, and it must be bigger than the size of the existing file system. If the new file system is not larger than the size of the existing file system, an error message is displayed, and no action is taken.</p> <p>This variable is used with the <code>Storage&gt; fs growto</code> command.</p>
length_change	<p>Expands the file system by a specified size. The size that you specify must be a positive number, and it must be lesser than the available space. If it exceeds the available space, an error message is displayed, and no action is taken.</p> <p>This variable is used with the <code>Storage&gt; fs growby</code> command.</p>
pool1[,disk1,...]	<p>Specifies the pool(s) or disk(s) to use for the file system. If you specify a pool or disk that does not exist, an error message is displayed, and the file system is not resized. You can specify more than one pool or disk by separating the name with a comma; however, do not include a space between the comma and the name.</p> <p>To find a list of existing pools and disks, use the <code>Storage&gt; pool list</code> command.</p> <p>To find a list of the existing disks, use the <code>Storage&gt; disk list</code> command.</p> <p>The disk needs to be part of the pool or an error message displays.</p>
protection	<p>The default value for the protection field is <code>disk</code>.</p> <p>Available options are:</p> <ul style="list-style-type: none"> <li>■ <code>disk</code> - if the protection is set to <code>disk</code>, then mirrors are created on separate disks. This flag only works for file systems of type <code>mirrored</code>, <code>mirrored-striped</code>, and <code>striped-mirror</code>. The disks may or may not be in the same pool.</li> <li>■ <code>pool</code> - if the protection is set to <code>pool</code>, then mirrors are created in separate pools. This flag only works for file systems of type <code>mirrored</code>, <code>mirrored-striped</code>, and <code>striped-mirror</code>. If not enough space is available, then the file system creation operation fails.</li> </ul>

## Decreasing the size of a file system

You can decrease (shrink) the size of the file system.

---

**Note:** For a scale-out file system, you can decrease the size of the primary tier only.

---

See [“About scale-out file systems”](#) on page 335.

To decrease the size of the file system, it must be online. If the file system is not online, an error message is displayed, and no action is taken.

You cannot decrease the size of a file system if a rollback exists. Delete the rollback first before using the `Storage> fs shrinkto` or `Storage> fs shrinkby` commands.

### **To decrease the size of a file system to a specified size**

- ◆ To decrease the size of a file system, enter the following:

```
Storage> fs shrinkto {primary|secondary} fs_name new_length
```

For example:

```
Storage> fs shrinkto primary fs1 10M
```

**To decrease the size of a file system by a specified size**

- ◆ To decrease the size of a file system, enter the following:

```
Storage> fs shrinkby {primary|secondary} fs_name length_change
```

For example:

```
Storage> fs shrinkby primary fs1 10M
```

primary   secondary	Specifies the primary or the secondary tier.
fs_name	Specifies the file system whose size decreases. If you specify a file system that does not exist, an error message is displayed.
new_length	Specifies the size to decrease the file system to. The size that you specify must be a positive number, and it must be smaller than the size of the existing file system. If the new file system size is not smaller than the size of the existing file system, an error message is displayed, and no action is taken.
length_change	Decreases the file system by a specified size. The size that you specify must be a positive number, and it must be smaller than the size of the existing file system. If the new file system size is not smaller than the size of the existing file system, an error message is displayed, and no action is taken.

---

**Note:** Decreasing the size of a file system can take a long time if there are many extents allocated in the shrink area, as these extents have to be relocated to other areas in the file system.

---

## About quotas for usage

Disk quotas limit the usage for users or user groups. You can configure disk quotas for file systems or for CIFS home directories.

---

**Note:** Quota works over NFS, but quota reporting and quota details are not visible over NFS.

---

Users and groups visible through different sources of name service lookup (nsswitch), local users, LDAP, NIS, and Windows users can be configured for file systems or CIFS home directory quotas.

There are two types of disk quotas:

- Usage quota (numspace) - limits the amount of disk space that can be used on a file system.  
The numspace quota value must be an integer with a unit. The minimum unit is KB, because the block size in the underlying Veritas File System (VxFS) is 1KB, and VxFS calculates numspace quotas based on the number of KBs. The range for numspace is from 1K to 9007199254740991( $2^{53} - 1$ )K.
- Inode quota (numinodes) - limits the number of inodes that can be created on a file system.  
An inode is a data structure in a UNIX or UNIX-like file system that describes the location of some or all of the disk blocks allocated to the file.  
The numinodes quota value must be an integer without a unit, and the range is from 1 to 999999999999999999(19bit).  
0 is valid for numspace and numinodes, which means the quota is infinite.

Veritas Access supports disk quota limits greater than 2 TB.

In addition to setting a limit on disk quotas, you can also define a warning level, or soft quota, whereby the Veritas Access administrator is informed that they are nearing their limit, which is less than the effective limit, or hard quota. Hard quota limits can be set so that a user is strictly not allowed to cross quota limits. A soft quota limit must be less than a hard quota limit for any type of quota.

---

**Note:** The alert for when a hard limit quota or a soft limit quota is reached in Veritas Access is not sent out immediately. The hard limit quota or soft limit quota alert is generated by a cron job scheduled to run daily at midnight.

---

## Enabling, disabling, and displaying the status of file system quotas

To configure file system quotas, you must enable the file system quotas. You can enable file system quotas for all file systems or specify a file system name. You can enable quotas per user (**userquota**), quotas per group (**groupquota**), or both.

Once the quotas are enabled, you set the values for the number of blocks or the number of inodes that can be created. Quotas can be hard limits or soft limits.

See [“Setting and displaying file system quotas”](#) on page 363.

### To enable a file system quota

- ◆ To enable a file system quota, enter the following:

```
Storage> quota fs enable [fs_name] [userquota | groupquota]
```

For example, to enable a quota (user and group) for file system `fs1`:

```
Storage> quota fs enable fs1
ACCESS quota SUCCESS V-288-0 userquota enabled for filesystem fs1
ACCESS quota SUCCESS V-288-0 groupquota enabled for filesystem fs1
```

### To disable a file system quota

- ◆ To disable a file system quota, enter the following:

```
Storage> quota fs disable [fs_name] [userquota | groupquota]
```

For example, to disable the user quota for file system `fs1`:

```
Storage> quota fs disable fs1 userquota
Command completed successfully
```

### To display the status of a file system quota

- ◆ To display the status of a file system quota, enter the following:

```
Storage> quota fs status [fs_name] [userquota | groupquota]
```

For example, to display the status of a file system quota (enabled or disabled):

```
Storage> quota fs status
FS name      User Quota  Group Quota
=====      =====
fsmirror     Disabled   Disabled
quotafs      Enabled    Enabled
striped1     Enabled    Enabled
fs1          Disabled   Enabled
Command completed successfully
```

---

**Note:** If the LDAP client is disabled, then the quota information may not be displayed using the `Storage> quota show` command for LDAP users and groups.

---

## Setting and displaying file system quotas

You can set usage quotas for users or for groups.

Before the file system quotas take effect, you must enable the quotas for the file system.

See [“Enabling, disabling, and displaying the status of file system quotas”](#) on page 361.

### To set the quota value

- ◆ To set the quota value for a file system, enter the following:

```
Storage> quota fs set {userquota | groupquota} user_or_group_names
domain_name [hardlimit | softlimit] [numinodes | numspace]
[value] [fs_name]
```

Domain name is the first section of the domain, for example:

```
veritas.example.com
```

The domain name is `veritas` in the example above.

If a value is not provided, the default value is used.

For example, to set the user quota (hardlimit and numinodes) of user `qtuser` on file system `fs1`:

```
Storage> quota fs set userquota qtuser qtomain hardlimit numinodes 200
ACCESS quota SUCCESS V-288-0 userquota for local\cifsuser has been set
with value 200 on filesystem
```

```
Storage> quota fs show fs1 userquota qtuser
```

User Quota Details for filesystem fs1:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
qtuser	0	0	0	0	0	957

OK Completed

**To set all quota values**

- ◆ To set all of the quota values, enter the following:

```
Storage> quota fs setall {userquota | groupquota}
[hardlimit | softlimit] [numinodes | numspace]
[value] [fs_name]
```

For example, to set all existing user quotas to default values:

```
Storage> quota fs show fs1
```

User Quota Details for filesystem fs1:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
a1	0	0	10G	0	1000	10000
qtuser	0	0	0	0	0	957
qtuser2	0	1000K	0	0	0	0

```
Storage> quota fs setall userquota
```

OK Completed

```
Storage> quota fs show fs1
```

User Quota Details for filesystem fs1:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
a1	0	0	10G	0	1000	1000
qtuser	0	0	0	0	0	1000
qtuser2	0	1000K	0	0	0	1000

**To display the file system settings**

- ◆ To display the file system settings, enter the following:

```
Storage> quota fs show [fs_name] [userquota | groupquota]
[user_or_group_names]
```

For example, to display quota values for the file systemx:

```
Storage> quota fs show
User Quota Details for filesystem quotas:
User      Space  Soft  Hard  Files  Soft  Hard
Name      Used   Space Space  Used   Files Files
=====  =====
quotauser 10M    1M    20M   1      5     1000
quotauser 9M     1M    10M   1      0      0
qtuser    10M   10M   20M   9      5     1000
qtuser2   19M   5M    20M   1      0     1000

User Quota Details for filesystem fs1:
User      Space  Soft  Hard  Files  Soft  Hard
Name      Used   Space Space  Used   Files Files
=====  =====
a1        0      0     10G   0      1000 1000
qtuser    0      0      0     0      0     1000
qtuser2   0     1000K 0      0      0     1000

User Quota Details for filesystem longfilesystemnameforqt:
User      Space  Soft  Hard  Files  Soft  Hard
Name      Used   Space Space  Used   Files Files
=====  =====
qtuser    0      0      0     0     901   1000
OK Completed
```

---

**Note:** If the LDAP client is disabled, then the quota information may not be displayed using the `Storage> quota show` command.

---

- fs\_name** File system name you want to set the quota for.
- userquota** User quota can be set with hard or soft limits on usage. Usage is dictated by the number of blocks and number of inodes that are created by the user.

groupquota	Group quota can be set with hard or soft limits on usage. Usage is dictated by the number of blocks and number of inodes that are created by all the users in the group.
user_or_group_names	Name of the user or the name of the group for which a quota value is set.  You can specify a comma-separated list of user or group names.  To delete quota values for a user, you have to set all the user quota entries to 0. A user with a UID of 0 is not allowed in a Storage> quota fs set command.

### To set the default quota values

- ◆ To set the default quota values, enter the following:

```
Storage> quota fs setdefault {userquota | groupquota}  
{hardlimit | softlimit} {numinodes | numspace} [value] [fs_name]
```

For example, to set the default group quota value:

```
Storage> quota fs setdefault groupquota hardlimit numspace 1T  
ACCESS quota SUCCESS V-288-0 default value of groupquota has been  
set with value 1T on filesystem
```

### To display the default values

- ◆ To display the default values, enter the following:

```
Storage> quota fs showdefault [fs_name] [userquota | groupquota]
```

For example, to display the default quota values:

```
Storage> quota fs showdefault
Default Quota values:
=====
Title           User/Group  Soft   Hard   Soft   Hard
                Quota      Space Space  Files  Files
=====
Default Quota  User Quota  -     -     -     1000
Default Quota  Group Quota -     1T    -     -

Per FS default Quota values:
=====
FS             User/Group  Soft   Hard   Soft   Hard
Name          Quota      Space Space  Files  Files
=====
fs1           User Quota  -     -     -     1000
OK Completed
```

## Setting user quotas for users of specified groups

You can set the same quota for each user in a group with a single command. As with the other quota commands, you can specify hard or soft limits. for the number of inodes or the usage space.

### To set user quotas for users of specified groups

- ◆ To set user quotas on users of specified groups, enter the following:

```
Storage> quota fs setbygroup group_names domain_name
[hardlimit | softlimit] [numinodes | numspace]
[value] [fs_name]
```

For example, to set the user quota for users of local groups:

```
Storage> quota fs setbygroup group1 local softlimit
numspace 50M fs1
ACCESS quota SUCCESS V-288-0 default value of  has been set with value 50M on
filesystem fs1
```

**Storage> quota fs show fs1**

User Quota Details for filesystem fs1:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
cifsuser	0	50M	0	1	198	6549

**Storage> cifs local group show cifsgrp1**

GroupName	UsersList
cifsgrp1	cifsusr2,cifsusr1

**Storage> cifs local group show cifsgrp2**

GroupName	UsersList
cifsgrp2	cifsusr3

For example, to set the user quota for users of the winbind group:

**Storage> quota fs setbygroup "domain users" javadom**

**hardlimit numspace 50M fs2**

OK Completed

**Storage> quota fs show**

User Quota Details for filesystem fs2:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
JAVADOM\administrator	0	0	50M	0	0	0
JAVADOM\krbtgt	0	0	50M	0	0	0
JAVADOM\support_388945a0	0	0	50M	0	0	0
JAVADOM\java	0	0	50M	0	0	0
JAVADOM\power	0	0	50M	0	0	0
JAVADOM\james	0	0	50M	0	0	0
JAVADOM\12345	0	0	50M	0	0	0
JAVADOM\space	0	0	50M	0	0	0

OK Completed

## About quotas for CIFS home directories

You use `Storage> quota cifshomedir` commands to configure quotas for CIFS home directories. Users and groups visible through different sources of name service

lookup (nsswitch), local users, LDAP, NIS, and Windows users can be configured for CIFS home directory quotas.

Default values are entered in a configuration file only. The actual application of the quota is done with the `set` and `setall` commands using the default values provided.

When a CIFS home directory file system is changed, quota information for a user's home directory is migrated from the existing home directory file system to the new home directory file system.

Quota migration results are based on the following logic:

- Case 1:

In the case where the existing home directory file system is NULL, you can set the new home directory file system to be multiple file systems (for example, fs1, fs2). If the multiple file systems previously had different quota values, the quota status and values from the first file system are migrated to other file systems in the new home directory. The first file system is the template. Only the user/group quota values that existed on the first file system are migrated. Other user/group quota values remain the same on the other file system.

For example, assume the following:

- The new home directory file systems are fs1 and fs2.
- user1, user2, and user3 have quota values on fs1.
- user2, user3, and user4 have quota values on fs2.

For the migration, user/group quota values for user1, user2, and user3 are migrated from fs1 to fs2. Quota values for user4 are kept the same on fs2, and user4 has no quota values on fs1.

- Case 2:

When the existing home directory file systems are already set, and you change the file systems for the home directory, the quota status and values need to be migrated from the existing home directory file systems to the new file systems. For this migration, the first file system in the existing home directory acts as the template for migrating quota status and values.

For example, if the existing home directory file systems are fs1 and fs2, and the file systems are changed to fs2, fs3, and fs4, then the user/group quota values on fs1 are migrated to fs3 and fs4. Other user/group values on fs3 and fs4 remain the same.

## Using quotas for CIFS home directories

### To set the default value used for quota limits for CIFS home directories

- ◆ To set the default value used for quota limits for CIFS home directories, enter the following:

```
Storage> quota cifshomedir setdefault {userquota | groupquota}
{hardlimit | softlimit} {numinodes | numspace} [value]
```

**userquota**            User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

**groupquota**            Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

**hardlimit**            Hard quota limit.

**softlimit**            Soft quota limit.

**numinodes**            Inode quota for the file system.

**numspace**            Usage quota for the file system.

**value**                Quota value for the users or groups on a file system.

If a value is not specified, then the value is 0.

If `Storage> quota fs setdefault` is set for particular file systems, then that default value has precedence.

If a value is 0 is entered, it is treated as an unlimited quota. If all values for a user or group quota are 0, the user or group is automatically deleted from the quota settings, which means that the `Storage> quota fs show` command will not show this user's or group's settings, as all quota values are treated as an unlimited quota.

For example, to set the default CIFS home directory user quota value:

```
Storage> quota cifshomedir setdefault userquota hardlimit
numspace 2T
```

```
ACCESS quota SUCCESS V-288-0 default value of userquota has been
set with value 2T on CIFS filesystems
```

**To display default quota values for CIFS home directories**

- ◆ To display the default quota values of the CIFS home directories, enter the following:

```
Storage> quota cifshomedir showdefault [userquota | groupquota]
```

```
userquota      User quota can be set with hard/soft limits on usage. Usage is
                dictated by the number of blocks and number of inodes that can
                be created by the user.
```

```
groupquota     Group quota can be set with hard/soft limits on usage. Usage is
                dictated by the number of blocks and number of inodes that can
                be created by all the users in the group.
```

For example, to display the 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	-		-	-	-

### To set a quota for CIFS home directories

- ◆ To set a quota for the user or group for CIFS home directories, enter the following:

```
Storage> quota cifshomedir set {userquota | groupquota}
user_or_group_names domainname [hardlimit | softlimit]
[numinodes | numspace] [value]
```

For example, to set the user quota (hardlimit and numinodes) of user `qtuser` on CIFS home directories:

```
Storage> quota cifshomedir set userquota cifsuser local
hardlimit numinodes 6549
```

```
ACCESS quota SUCCESS V-288-0 userquota for local\cifsuser has been
set with value 6549 on CIFS filesystems
```

```
Storage> quota cifshomedir show
```

```
User Quota Details for CIFS homedirfs:
```

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
qtuser	0	20M	100M	0	1000	6549

- userquota** User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.
- groupquota** Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.
- user\_or\_group\_names** Name of the user or the name of the group for which a quota value is set.  
 You can specify a comma-separated list of user or group names.  
 To delete quota values for a user, you will have to set all the user quota entries to 0.  
 A user with a UID of 0 is not allowed in a `Storage> quota fs set` command.
- domainname** Domain name is the first section of the domain.  
 For example, in  
`veritas.access.com`  
 the domain name is `veritas`.
- hardlimit** Hard quota limit.

softlimit	Soft quota limit.
numinodes	Inode quota for the file system.
numspace	Usage quota for the file system.
value	<p>Quota value for the CIFS home directories.</p> <p>If a value is not provided, the default value set from using the <code>Storage&gt; quota fs setdefault</code> command is used.</p> <p>If <code>Storage&gt; quota fs setdefault</code> is set for particular file systems, then that default value has precedence.</p> <p>If a value is 0 is entered, it is treated as an unlimited quota. If all values for a user or group quota are 0, the user or group is automatically deleted from the quota settings, which means that the <code>Storage&gt; quota fs status</code> command will not show this user's or group's settings, as all quota values are treated as an unlimited quota.</p>

**To set the quota value for all users and groups**

- ◆ To set the quota value for all users and groups for whom the quota has already been set with the `set` commands, enter the following:

```
Storage> quota cifshomedir setall {userquota | groupquota}
[hardlimit | softlimit] [numinodes | numspace]
[value]
```

Other users and groups (for whom quota has not been set previously) will not be affected.

For example, to set all existing user quotas for CIFS home directories:

```
Storage> quota cifshomedir show
```

User Quota Details for CIFS homedirfs:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
qtuser	0	20M	100M	0	1000	6549

```
Storage> quota cifshomedir setall userquota softlimit
numinodes 198
```

ACCESS quota SUCCESS V-288-0 userquota has been set with value 198 on CIFS filesystems for all the existing users/groups

```
Storage> quota cifshomedir show
```

User Quota Details for CIFS homedirfs:

User Name	Space Used	Soft Space	Hard Space	Inodes Used	Soft Inodes	Hard Inodes
qtuser	0	20M	100M	0	198	6549

- userquota User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.
- groupquota Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.
- hardlimit Hard quota limit.
- softlimit Soft quota limit.
- numinodes Inode quota for the file system.

**numspace** Usage quota for the file system.

**value** Quota value for CIFS home directories for whom the quota has already been set with `set` commands.

If a value is not provided, the default value set from using the `Storage> quota fs setdefault` command is used.

If `Storage> quota fs setdefault` is set for particular file systems, then that default value has precedence.

If a value is 0 is entered, it is treated as an unlimited quota. If all values for a user or group quota are 0, the user or group is automatically deleted from the quota settings, which means that the `Storage> quota fs status` command will not show this user's or group's settings, as all quota values are treated as an unlimited quota.

### To enable the quota for CIFS home directories

- ◆ To enable the quota for CIFS home directories, enter the following:

```
Storage> quota cifshomedir enable [userquota | groupquota]
```

**userquota** User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

**groupquota** Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

For example, to enable quotas (user and group quotas) for CIFS home directories:

```
Storage> quota cifshomedir enable
```

```
ACCESS quota SUCCESS V-288-0 userquota enabled for filesystem fs1
```

### To disable the quota for CIFS home directories

- ◆ To disable the quota for the CIFS home directories, enter the following:

```
Storage> quota cifshomedir disable [userquota | groupquota]
```

userquota            User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

groupquota           Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

For example, to disable the group quota for CIFS home directories:

```
Storage> quota cifshomedir disable groupquota
```

```
ACCESS quota SUCCESS V-288-0 groupquota disabled for filesystem fs1
```

### To display the status of the quota for CIFS home directories

- ◆ To display the quota status of the CIFS home directories, enter the following:

```
Storage> quota cifshomedir status [userquota | groupquota]
```

Displays only if the quota is enabled or disabled.

userquota            User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

groupquota           Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

For example, to display the status of a CIFS home directory quota (enabled or disabled):

```
Storage> quota cifshomedir status
```

FS name	User Quota	Group Quota
=====	=====	=====
CIFS homedirectories	Enabled	Disabled

## Displaying the quota values for CIFS home directories

### To display the quotas for CIFS home directories

- ◆ To display the quotas for the CIFS home directories, enter the following:

```
Storage> quota cifshomedir show [userquota | groupquota]
[user_or_group_names]
```

**userquota** User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

**groupquota** Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

**user\_or\_group\_names** Name of the user or the name of the group for which a quota value is set.

You can specify a comma-separated list of user or group names.

To delete quota values for a user, you will have to set all the user quota entries to 0.

A user with a UID of 0 is not allowed in a `Storage> quota fs set` command.

For example, to display general quota information for a CIFS home directory for both `userquota` and `group quota`:

```
Storage> quota cifshomedir show
User Quota Details for CIFS homedirfs:
User Name Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====
user06 0 30M 50M 0 0 0
user07 0 0 0 0 300 500
Group Quota Details for CIFS homedirfs:
Group Name Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====
group01 0 400M 600M 0 0 0
group02 0 0 0 0 60000 80000
```

The `Storage> quota cifshomedir show` command does not display the file system name in the output.

The CIFS home directory is created on one of the CIFS home directory file systems. Veritas Access sets CIFS home directory quotas on all of the CIFS home directory file systems. The `Storage> quota cifshomedir show userquota username` command displays the quota and usage information on the file system on which the CIFS home directory is created.

For example, if `homedirfs=fs1,fs2`, and the home directory of user1 is created on fs1, and the home directory of user2 is created on fs2, then the `Storage> quota cifshomedir show userquota user2` command displays the CIFS home directory quota and usage on fs2.

**To display the quota values that are already set on each file system for the CIFS home directories**

- ◆ To display the quota values that are already set on each file system for the CIFS home directories, enter the following:

```
Storage> quota cifshomedir showdetail [userquota | groupquota]
[user_or_group_names]
```

**userquota** User quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by the user.

**groupquota** Group quota can be set with hard/soft limits on usage. Usage is dictated by the number of blocks and number of inodes that can be created by all the users in the group.

**user\_or\_group\_names** Name of the user or the name of the group for which a quota value is set.

You can specify a comma-separated list of user or group names.

To delete quota values for a user, you will have to set all the user quota entries to 0.

A user with a UID of 0 is not allowed in a `Storage> quota fs set` command.

For example, to display quota information on CIFS home directory file systems `fs1` and `fs2` for both `userquota` and `groupquota`:

```
Storage> quota cifshomedir showdetail
User Quota Details for filesystem fs1:
User Name  Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====  =====  =====  =====  =====  =====  =====  =====
user06     0           30M       50M       0           0           0           0
user07     0           0         0         0           0           300         500
User Quota Details for filesystem fs2:
User Name  Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====  =====  =====  =====  =====  =====  =====  =====
user06     0           30M       50M       0           0           0           0
user07     0           0         0         0           0           300         500
Group Quota Details for filesystem fs1:
Group Name  Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====  =====  =====  =====  =====  =====  =====  =====
group01     0           400M     600M     0           0           0           0
group02     0           0         0         0           0           60000       80000
Group Quota Details for filesystem fs2:
Group Name  Space Used Soft Space Hard Space Inodes Used Soft Inodes Hard Inodes
=====  =====  =====  =====  =====  =====  =====  =====
group01     0           400M     600M     0           0           0           0
group02     0           0         0         0           0           60000       80000
```

The file system name displays in the output for the `Storage> quota cifshomedir showdetail` command.

## Managing a file system

### Defragmenting a file system

You can either defragment a file system now or you can schedule a defragment job for a file system.

#### To defragment a file system

- ◆ To defragment a file system, enter the following:

```
Storage> fs defrag now fs_name time [defrag_level]
```

*fs\_name* Specifies the name of the file system that you want to defragment.

**Note:** The specified file system must be online before attempting to defragment the file system.

*time* Specifies the maximum time to run. The defragmentation options are processed until defragmentation is complete, or until the time limit expires. The time value should be larger than one minute.

Potential time value output and what the values mean:

- 10M - indicates 10 minutes
- 1H20M - indicates 1 hour and 20 minutes
- Infinite - indicates the defragmentation process continues to run until the defragmentation process is done completely.

There is no limit time.

*defrag\_level* Specifies the defragmentation level such as `dir`, `extent`, or `all`.

For example:

```
Storage> fs defrag now fs1 1H20M
```

It will take some time to do the defragmentation

do you want to continue? yes|no

**y**

**To schedule a defragment job for a file system.**

**1** Create a defrag schedule job for a file system that reoccurs once a week:

```
Storage> fs defrag schedule create sched_name sched_duration \
minute [hour] [day_of_the_month] \
[month] [day_of_the_week]
```

- sched\_name* Specifies the the name of the schedule.
- sched\_duration* Specifies the duration of the defragmenatation job.
- minute* Specifies the minute (0-59).
- hour* Specifies the hour (0-23).
- day\_of\_the\_month* Specifies the day of the month (1-31).
- month* Specifies the month of the year (1-12).
- day\_of\_the\_week* Specifies the day of the week (0-6 with 0=Sunday).

For example:

Create a defrag schedule called `schedule1` that runs at 11:00 pm every Saturday for a duration of 2 hours.

```
Storage> fs defrag schedule create schedule1 2 0 23 * * 6
ACCESS defrag Success V-288-999 Defrag Schedule creation succeeded
```

The number `2` after `schedule1` is the duration of how long the defrag schedule will run. `0` indicates minutes and `23` is the hour for which the defrag schedule will run.

**2** Show the defrag schedule details:

```
Storage> fs defrag schedule show sched_name
```

For example:

Show the defrag schedule details of `schedule1`:

```
Storage> fs defrag schedule show schedule1
Schedule Information for schedule1
=====
Name      Node      Duration Minute Hour Day Month WeekDay
=====
schedule1 mtvna_01 8hours   15     23  *   *     6
```

**3 Start the defrag schedule job for a file system:**

```
Storage> fs defrag schedule start fs_name sched_name
```

For example

Start the defrag `schedule1` schedule job for `tpcc_data1` file system:

```
Storage> fs defrag schedule start tpcc_data1 schedule1
ACCESS defrag SUCCESS V-288-999 starting schedule1 for fsname
tpcc_data1
```

**4 List the scheduled defrag job status for a file system:**

```
Storage> fs defrag schedule list fs_name
```

For example:

List the scheduled defrag job status for `tpcc_data1` file system :

```
Storage> fs defrag schedule list tpcc_data1
Schedule Information for tpcc_data1
=====
Name      Node      Duration Minute Hour Day Month WeekDay
=====
schedule1 mtvnas_01 8hours   15      23   *   *       6
```

## Modifying the scheduled defragmentation

### To modify the scheduled defragmentation

**1 Stops the schedule for the file system:**

```
Storage> fs defrag schedule stop fs_name
```

where `fs_name` is the name of the file system.

For example:

```
Storage> fs defrag schedule stop tpcc_data1
```

**2 Remove specified schedule:**

```
Storage> fs defrag schedule remove new_schedule
```

For example:

```
Storage> fs defrag schedule remove schedule1
```

### 3 Create a scheduled defragmentation:

```
Storage> fs defrag schedule create new_schedule
      duration
      min \
      [hour] [day_of_month] [month] [day_of_week] [node]
```

where *new\_schedule* is the name of the schedule.

where *duration* is the duration specified in hours (1 or more).

where *min* is the minutes.

where *hour* is the hours.

where *day* is the day of the month.

where *month* is the month.

where *day\_of\_week* is the day of the week.

where *node* is the name of the node or you can use "any".

For example:

```
Storage> fs defrag schedule create schedule2 3 0 2 * * 6
```

This creates a schedule called "schedule2" that starts defragmentation at 2:00 am every Saturday and runs for only 3 hours.

### 4 Start the schedule for a given file system:

```
Storage> fs defrag schedule start fs_name
```

For example:

```
Storage> fs defrag schedule start fs1
```

## Removing the specified schedule

### To remove the specified schedule

#### ◆ Remove the specified schedule:

```
Storage> fs defrag schedule remove new_schedule
```

where *new\_schedule* is the name of the schedule.

For example:

```
Storage> fs defrag schedule remove schedule1
```

## Stopping the schedule for a file system

### To stop the schedule for a file system

- ◆ Stop the schedule for a file system:

```
Storage> fs defrag schedule stop fs_name
```

where *fs\_name* is the name of the file system.

For example:

```
Storage> fs defrag schedule stop tpcc_data1
```

## Checking and repairing a file system

The `Storage> fs fsck` command lets you check and repair a file system while the file system is offline.

The `Storage> fs fsck` command tries to perform a normal fsck (check and repair) of the file system first, but if the `fullfsck` option is set, the command proceeds depending on the input that is provided by the user.

In most cases, a normal fsck (only log replay) is sufficient to repair a file system. In cases where there is structural damage to the file system's metadata, a full fsck of the file system may be necessary to repair the file system.

---

**Warning:** Using the `Storage> fs fsck` command on an online file system can damage the data on the file system. Only use the `Storage> fs fsck` command on a file system that is offline.

---

---

**Note:** When running the `Storage> fs fsck` command, you may encounter a process of `Unknown`. The `Unknown` process is normal, since there is no process printed as output when running a normal fsck using `Storage> fsck fs_name`. Full fsck is run only if the normal fsck fails. In the support mode, if you are running a full fsck, Veritas Access records that status in an internal database/file.

---

### To check and repair a file system

- ◆ To check and repair a file system, enter the following:

```
Storage> fs fsck fs_name
```

where *fs\_name* specifies the file system for which you want to check and repair.

For example:

```
Storage> fs fsck fs1
Do you want to do fsck without log replay? yes|no
n
File system fs1 fsck successfully
```

## About scale-out fsck

The scale-out fsck operation does the following:

- Checks the consistency of the metadata container, the data container, and the database, and repairs any inconsistencies.
- Checks if the metadata container and the data container are marked for full fsck. If yes, scale-out fsck performs a full fsck of the corresponding file systems. Based on the actions taken by fsck on the individual file systems, the scale-out fsck operation repairs the inconsistencies in other parts of the scale-out file system.  
See [“About scale-out file systems”](#) on page 335.
- Goes through all the file handles present in the database, and checks if the corresponding metadata container and the data container file handles are consistent with each other.

In some cases, full fsck might delete files from the data container. To maintain consistency, the corresponding files from the metadata container and the data container are removed, and the corresponding key is removed from the database.

```
Storage> fs fsck fs1
fsck of largefs fs1 is successful
```

## Configuring FastResync for a file system

If the power fails or a switch fails, mirrors in a file system may not be in a consistent state.

The `Storage> fs setfastresync(FastResync)` command performs quick and efficient resynchronization of stale mirrors.

---

**Note:** You must have at least two mirrors on the file system to enable FastResync.

---

### To enable the FastResync option

- ◆ To enable FastResync for a file system, enter the following:

```
Storage> fs setfastresync fs_name [pool_or_disk_name]
```

**fs\_name** Specifies the name of the file system for which to enable FastResync.

**pool\_or\_disk\_name** Specifies the pool or the disk name to resynchronize from the mirrored file system that spans the specified pool or disk.

For example, to enable FastResync for a file system, enter the following:

```
Storage> fs setfastresync fs6
```

You can also enable FastResync for a tier of a file system.

```
Storage> tier setfastresync fs_name [pool_or_disk_name]
```

**fs\_name** Specifies the name of the file system for which to enable FastResync.

**pool\_or\_disk\_name** Specifies the pool or the disk name to resynchronize from the mirrored file system that spans the specified pool or disk.

## Disabling the FastResync option for a file system

You can disable the FastResync option for a file system.

---

**Note:** When instant rollbacks exist for a volume, you cannot disable the FastResync option for a file system.

---

### To disable the FastResync option

- ◆ To disable the FastResync option for a file system, enter the following:

```
Storage> fs unsetfastresync fs_name
```

where:

*fs\_name* Specifies the name of the file system for which to disable FastResync. If you specify a file system that does not exist, an error message is displayed.

For example:

```
Storage> fs unsetfastresync fs6
```

You can also disable FastResync for a tier of a file system.

```
Storage> tier unsetfastresync fs_name
```

where:

*fs\_name* Specifies the name of the file system for which to disable FastResync. If you specify a file system that does not exist, an error message is displayed.

## Checking and resynchronizing stale mirrors

You can check if there is a stale mirror on any of your file systems. If there is a stale mirror, the stale mirror needs to be resynchronized, and the resynchronization process needs to be verified.

### To check if there are stale mirrors on your file systems

- ◆ To check if your file systems contain a stale mirror, enter the following:

```
Storage> fs checkmirror
```

For example, to display the file systems that have a stale mirror, enter the following:

```
Storage> fs checkmirror
fs_name:
-----
mirror3
```

**To resynchronize all stale mirrors or a stale mirror for a specified file system**

- ◆ To resynchronize all stale mirrors or a stale mirror for a specified file system, enter the following:

```
Storage> fs resync [fs_name]
```

where *fs\_name* is the name of the specified file system where you want to resynchronize for stale mirrors.

If you do not include *fs\_name*, you resynchronize all the stale mirrors for all your file systems.

For example, to resynchronize all stale mirrors for all file systems, enter the following:

```
Storage> fs resync
```

```
Resync stale mirror for file systems are started in background.
```

For example, to resynchronize all stale mirrors for a specified file system, enter the following:

```
Storage> fs resync mirror3
```

```
Resync stale mirror for file system mirror3 is started in  
background.
```

**To verify the resynchronization process for your stale mirrors**

- ◆ To verify the resynchronization process for your stale mirrors, enter the following:

```
Storage> fs checkresync
```

For example, to display the resynchronization progress running in the background, enter the following:

```
Storage> fs checkresync
```

FS	MIRROR	TYPE	PROGRESS	START_TIME	WORK_TIME
alltask_roll	tier 1	ROLLBACK	0.16%	Jun/20/2011/19:12:45	0:0:3
alltask_roll	tier 2	ROLLBACK	0.29%	Jun/20/2011/19:12:45	0:0:3
alltask	tier 1,mirror 02	RESYNC	1.56%	Jun/20/2011/21:20:02	0:4:18
alltask	tier 2,mirror 02	RESYNC	0.21%	Jun/20/2011/21:33:20	0:0:4
fsrelayout	tier 1	RELAYOUT	0.04%	Jun/20/2011/21:48:02	0:26:15
fsrelayout	tier 2	RELAYOUT	9.44%	Jun/20/2011/21:48:28	0:25:49

```

REMAINING_TIME
=====
30:29
17:01
4:30:54
32:03
1119:33:44
4:07:40

```

---

**Note:** If a column addition to a file system is in progress, the output of the `Storage> fs checkresync` command will include RELAYOUT status.

---

## Setting file system alerts

For a file system to run efficiently, you should always reserve some space for the file system rather than using 100% of the space. You can set file system alerts based on file system or snapshot usage. You can set the alert based on the number of inodes used, file system space used, or snapshot usage.

File system alerts can be displayed by using the `Report> showevents` command.

### To set file system alerts

- ◆ To set file system alerts, enter the following:

```
Storage> fs alert set numinodes | numspace | fullspace | fullinodes
value [fs_name,...] [snapshot_name]
```

numinodes	When setting the alert for <code>numinodes</code> , <code>value</code> is the number of inodes used. The default alert value for <code>numinodes</code> is set at 0. An alert will not be sent until you set it to a different value.
numspace	When setting the alert for <code>numspace</code> , <code>value</code> is the percentage you want to set to trigger the alert. By default, the alert is sent at 80%. If you do not specify a file system name, the default value is modified.
fullspace	<code>fullspace</code> is the tunable for setting an alert if the file system becomes full. When file system usage is above the limit set by the <code>fullspace</code> tunable, all the NFS/CIFS shares on the file system are automatically changed to read-only to prevent the file system from becoming full again. When you grow the file system or delete some files to free up space, the NFS/CIFS shares are automatically changed back to read-write (there might be a delay of up to five minutes) for the change to occur.  <b>Note:</b> The file system size is checked every five minutes. During this five-minute interval, if the usage of the file system grows to more than 80%, the NFS/CIFS shares are changed to read-only. If the file system is small and write I/O is fast, then the file system can be filled up to 100% before being changed to read-only. This is by design.  By default, the <code>fullspace</code> tunable is set to 0, which means that the <code>fullspace</code> tunable is disabled.
fullinodes	<code>fullinodes</code> is the tunable for setting an alert if the file system becomes full. When inodes on a file system reach the limit of <code>fullinodes</code> , the NFS/CIFS shares on the file system are automatically changed to read-only. After the file system is changed to read-only, you need to delete some files from the file system, and a remount of the file system may be required for the NFS/CIFS shares to be changed to read-write. By default, the <code>fullinodes</code> tunable is set to 0, which indicates that the <code>fullinodes</code> tunable is disabled.
fs_name	Name of the file system for which you want to set the file system alerts. <code>fs_name</code> is optional. To specify multiple file systems, use commas to separate the file system names.
snapshot_name	Name of the snapshot for which you want to set the file system alert.

**Note:** The following are reserved words for `snapshot_name`: `flags`, `ctime`, and `mtime`.

#### Examples of alerts:

**NUMSPACE alerts in** `Report> showevents`

```
2011 Nov 14 23:55:02 [CLUS_01,alert,master] [[fs alert]] numspace
set at 70(%) crossed for File System fs1, current usage 98(%)
```

NUMINODES alert in Report> showevents

```
2011 Nov 15 00:05:22 [CLUS_01,alert,master] [[fs alert]] numinodes
set at 2000 crossed for File System fs1, current usage 7768
```

Examples for setting alerts that are file-system specific:

```
Storage> fs alert set numinodes 2M fs1
ACCESS fs SUCCESS V-288-663 Alert of type [ numinodes ] set to 2M on
the file system fs1
```

```
Storage> fs alert set numinodes 2M
ACCESS fs SUCCESS V-288-663 Default Alert on the file systems of type
[ numinodes ] set to 2M
```

Examples for default alerts:

```
Storage> fs alert set numspace 80 fs1
ACCESS fs SUCCESS V-288-663 Alert of type [ numspace ] set to 80 on
the file system fs1
```

```
Storage> fs alert set numspace 60
ACCESS fs SUCCESS V-288-663 Default Alert on the file systems of
type [ numspace ] set to 60
```

Example for setting a fullspace alert:

```
Storage> fs alert set fullspace 98
ACCESS fs SUCCESS V-288-1805 Default Alert on the file systems of
type [ fullspace ] set to 98
Storage> fs alert unset fullspace
ACCESS fs SUCCESS V-288-1740 Alert of type [ fullspace ] set
to default value 0 (%)
```

Example for setting a fullinodes alert:

```
storage> fs alert set fullinodes 50000000
ACCESS fs SUCCESS V-288-1805 Default Alert on the file systems of type
[ fullinodes ] set to 50000000
```

```
Storage> fs alert show
```

File System	Alert Type	Value	Current Usage
fs2	numspace	85% (D)	75%
fs2	numinodes	0 (D)	110215
fs2	fullspace	98% (D)	75%

```
fs2          fullinodes    50000000 (D)    110215
share1      numspace      85% (D)        80%
share1      numinodes     0 (D)          8044
share1      fullspace    98% (D)        80%
share1      fullinodes    50000000 (D)    8044
```

## Displaying file system alert values

You can display the current disk space usage and the set alert value. A **D** beside the value indicates that the value is the default value used throughout the system.

### To display file system alert values

- ◆ To display file system alert values, enter the following:

```
Storage> fs alert show
```

For example:

```
Storage> fs alert show
File System      Alert Type  Value      Current Usage
=====
fs0              numspace   80% (D)    2%
fs0              numinodes  6500       1000
fs0              fullspace  98% (D)    2%
fs0              fullinodes 0 (D)      110215
fs1              numspace   80% (D)    2%
fs1              numinodes  8000       10000
fs1              fullspace  98% (D)    2%
fs1              fullinodes 0 (D)      115
fs4              numspace   80 (D)%    3%
fs4              numinodes  2000000 (D) 4
fs4              fullspace  98% (D)    3%
fs4              fullinodes 0 (D)      3155
```

## Removing file system alerts

You can remove the alerts set on a file system. If you remove an alert on any file system, you receive alerts for the file systems based on the default values.

### To remove file system alerts

- ◆ To remove file system alerts, enter the following:

```
Storage> fs alert unset numinodes | numspace | fullspace | fullinodes  
[fs_name,...] [snapshot_name]
```

**fs\_name** Name of the file system for which you want to remove the file system alert. *fs\_name* is optional.

When the fullspace/fullinodes tunables are unset (set to 0), the shares that were changed to read-only due to file system high usage are changed back to read-write mode immediately.

**snapshot\_name** Name of the snapshot for which you want to remove the file system alert.

**Note:** The following are reserved words for *snapshot\_name*: *flags*, *ctime*, and *mtime*.

See “[Setting file system alerts](#)” on page 389.

Examples for removing alerts that are file-system specific:

```
Storage> fs alert unset numinodes fs1  
ACCESS fs SUCCESS V-288-663 Alert of type [ numinodes ] set to DEFAULT  
value on the file system fs1
```

```
Storage> fs alert unset numspace fs1  
ACCESS fs SUCCESS V-288-663 Alert of type [ numspace ] set to DEFAULT  
value on the file system fs1
```

Examples of default alerts for removing alerts:

```
Storage> fs alert unset numinodes  
ACCESS fs SUCCESS V-288-663 Alert of type [ numinodes ] set to  
Default value 0
```

```
Storage> fs alert unset numspace  
ACCESS fs SUCCESS V-288-663 Alert of type [ numspace ] set to  
Default value 80 (%)
```

## Destroying a file system

The `Storage> fs destroy` command unmounts a file system and releases its storage back to the storage pool. You cannot destroy the file systems that CIFS or NFS share.

### To destroy a file system

- ◆ To destroy a file system, enter the following:

```
Storage> fs destroy fs_name
```

where *fs\_name* specifies the name of the file system that you want to destroy.

For example:

```
Storage> fs destroy fs1  
100% [#] Destroy filesystem
```

## Upgrading disk layout versions

In this release, you can create and mount only file systems with disk layout Version 8 and above.

## To upgrade the disk layout versions

- 1 Ensure the file system is online before proceeding.

You can find information about the file system version, enter the following:

```
Storage> fs list file_system_name
```

Sample output of the file system layout prior to upgrading the file system version:

```
Storage> fs list fs1
General Info:
=====
Block Size:      1024 Bytes
Layout:          Version 10
ACCESS_CLUST11_01:      online
ACCESS_CLUST11_02:      online
```

```
Primary Tier
=====
Size:            5.00G
Use%:            1%
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_0
```

```
Defrag Status: Not Running
Fullfsck Status: Not Running
Resync Status: Not Running
Rollsync Status: Not Running
Relayout Status: Not Running
```

**2 To upgrade a file system to the current layout, enter the following:**

```
Storage> fs upgrade file_system_name
```

For example:

```
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 11.
```

**Sample output of the file system layout after successfully upgrading the file system version:**

```
General Info:
```

```
=====
```

```
Block Size:      1024 Bytes
```

```
Version:         Version 11
```

```
ACCESS_CLUST11_01:      online
```

```
ACCESS_CLUST11_02:      online
```

```
Primary Tier
```

```
=====
```

```
Size:           5.00G
```

```
Use%:           1%
```

```
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_0
```

```
Defrag Status:  Not Running
```

```
Fullfsck Status: Not Running
```

```
Resync  Status:  Not Running
```

```
Rollsync Status: Not Running
```

```
Relayout Status: Not Running
```

**The following examples show unsuccessful upgrades:**

```
Storage> fs upgrade fs1
```

```
ACCESS fs ERROR V-288-2471 File system fs1 is already at upgraded  
version 11.
```

```
Storage> fs upgrade fssim
```

```
ACCESS fs ERROR V-288-685 fssim must be online to perform upgrade  
operation.
```

# Creating shares for applications

This chapter includes the following topics:

- [About file sharing protocols](#)
- [About concurrent access](#)
- [Sharing directories using CIFS and NFS protocols](#)
- [About concurrent access with NFS and S3](#)

## About file sharing protocols

Veritas Access provides support for multiple file sharing protocols. Veritas Access offers unified access, which provides the option to share a file system or a directory in a file system with more than one protocol. For unified access, only certain protocols combinations are supported.

See [“About concurrent access”](#) on page 399.

**Table 22-1** Protocols

Protocol	Definition
Amazon S3	The object access service lets you store and retrieve the data that is stored in Veritas Access using the Amazon Simple Storage Service (Amazon S3) protocol.  See <a href="#">“About the object access service”</a> on page 230.

**Table 22-1** Protocols (*continued*)

Protocol	Definition
CIFS	CIFS is active on all nodes within the Veritas Access cluster. The specific shares are read/write on the node they reside on, but can failover to any other node in the cluster. Veritas Access supports CIFS home directory shares.  See <a href="#">“About configuring Veritas Access for CIFS”</a> on page 156.
FTP	Allows clients to access files on Veritas Access servers.  See <a href="#">“About FTP”</a> on page 239.
NFS	All the nodes in the cluster can serve the same NFS share at the same time in read-write mode. This creates very high aggregated throughput rates, because you can use the sum of the bandwidth of all the nodes. Cache-coherency is maintained throughout the cluster.  Veritas Access supports both the NFS kernel-based server and the NFS-Ganesha server in a mutually exclusive way.  See <a href="#">“About using NFS server with Veritas Access”</a> on page 141.
Oracle Direct NFS	Optimized NFS client that provides faster access to NFS storage located on NAS storage devices.  See <a href="#">“About using Veritas Access with Oracle Direct NFS”</a> on page 285.

## About concurrent access

Veritas Access provides support for multi-protocol file sharing where the same file system can be exported to both Windows and UNIX users using the Common Internet File System (CIFS), Network File System (NFS) and Simple Storage Service (S3) protocols. The result is an efficient use of storage by sharing a single data set across multiple application platforms.

---

**Note:** When a share is exported over both NFS and CIFS protocols, the applications running on the NFS and CIFS clients may attempt to concurrently read or write the same file. This may lead to unexpected results, such as reading stale data, since the locking models used by these protocols are different. For this reason, Veritas Access warns you when the share export is requested over NFS or CIFS and the same share has already been exported for write access over CIFS or NFS.

---

The following sections describe concurrent access with multiple protocols.

See [“Sharing directories using CIFS and NFS protocols”](#) on page 400.

See “About concurrent access with NFS and S3” on page 403.

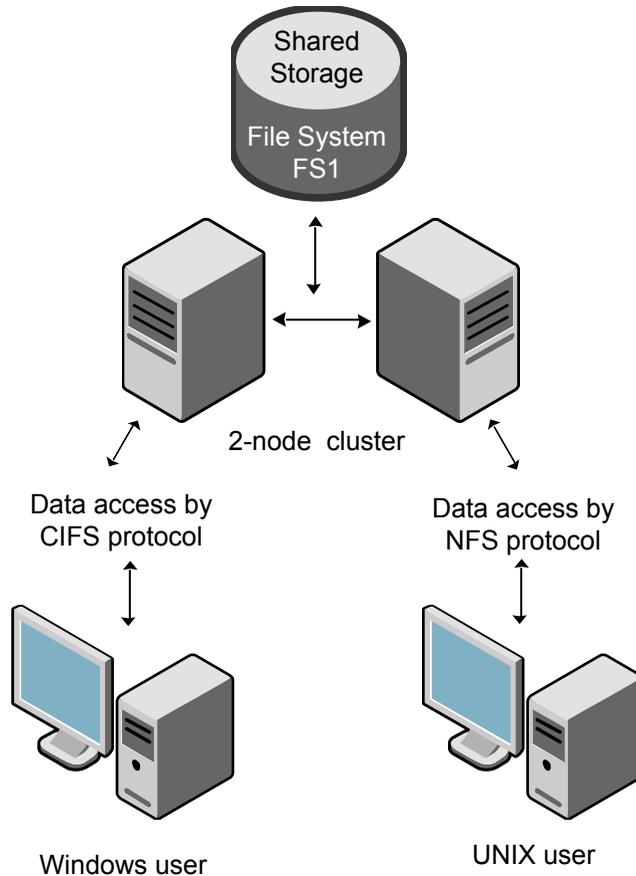
See “About file sharing protocols” on page 398.

## Sharing directories using CIFS and NFS protocols

Veritas Access provides support for multi-protocol file sharing where the same directory or file system can be exported to both Windows and UNIX users using the CIFS and NFS protocols. The result is an efficient use of storage by sharing a single data set across multi-application platforms.

Figure 22-1 shows how the directory sharing for the two protocols works.

**Figure 22-1** Exporting and/or sharing CIFS and NFS directories



---

**Note:** When a share is exported over both NFS and CIFS protocols, the applications running on the NFS and CIFS clients may attempt to concurrently read or write the same file. This may lead to unexpected results since the locking models used by these protocols are different. For example, sharing an export over both CIFS and NFS in read-write mode may lead to data corruption. For this reason, Veritas Access warns you when the share export is requested over NFS or CIFS in read-write mode, and is already being exported over CIFS or NFS in read-write mode.

---

It is recommended that you disable the `oplocks` option when the following occurs:

- A file system is exported over both the CIFS and NFS protocols.
- Either the CIFS and NFS protocol is set with read and write permission.

**To export a directory to Windows and UNIX users**

- 1** To export a directory to Windows and UNIX users with read-only and read-write permission respectively, enter the `CIFS` mode and enter the following commands:

```
CIFS> show
                Name  Value
                ----  -
netbios name   Pei60
ntlm auth      yes
allow trusted domains no
homedirfs
aio size       0
idmap backend  rid:10000-1000000
workgroup      PEI-DOMAIN
security       ads
                Domain PEI-DOMAIN.COM
                Domain user Administrator
                Domain Controller 10.200.107.251
                Clustering Mode normal
CIFS> share add fs1 share1 ro
Exporting CIFS filesystem : share1...
CIFS> share show
ShareName FileSystem ShareOptions
share1 fs1 owner=root,group=root,ro
```

**Exit CIFS mode:**

```
CIFS> exit
```

- 2** Enter the `NFS` mode and enter the following commands:

```
NFS> share add rw fs1
ACCESS nfs WARNING V-288-0 Filesystem (fs1)
is already shared over CIFS with 'ro' permission.
Do you want to proceed (y/n): y
Exporting */vx/fs1 with options rw
..Success.
NFS> share show
/vx/fs1 * (rw)
```

## Sharing a file system as a CIFS home directory

When the file system in CIFS is set to `homedirfs`, the Veritas Access software assumes that the file system is exported to CIFS users in read and write mode. Veritas Access does not allow you to export the same file system as an CIFS share and a home directory file system (`homedirfs`). For example, if the file system `fs1` is already exported as a CIFS share, then you cannot set it as `homedirfs`.

### To export a file system set as `homedirfs`

- ◆ To request that a file system be used for home directories, you need to export the file system. Go to the `CIFS` mode and enter the following:

```
CIFS> share show
ShareName      FileSystem  ShareOptions
share1         fs1        owner=root,group=root,rw
CIFS> set homedirfs fs1
ACCESS cifs ERROR V-288-615 Filesystem (fs1) is already exported
by another CIFS share.
```

## About concurrent access with NFS and S3

Veritas Access supports concurrent access to a shared file system or a directory from both NFS and S3. The supported configurations are:

- Applications or users write data to NFS shares, while other applications or users read the data over S3.
- Applications or users write data to S3 shares, while other applications or users read the data over NFS.

# Creating and maintaining NFS shares

This chapter includes the following topics:

- [About NFS file sharing](#)
- [Displaying file systems and snapshots that can be exported](#)
- [Exporting an NFS share](#)
- [Exporting an NFS share for Kerberos authentication](#)
- [Displaying exported directories](#)
- [About managing NFS shares using netgroups](#)
- [Configuring netgroups](#)
- [Exporting an NFS snapshot](#)
- [Unexporting a directory or deleting NFS options](#)

## About NFS file sharing

The Network File System (NFS) protocol enables exported directories (including all files under the directory that reside on the exported directory's file system) hosted by an NFS server to be accessed by multiple UNIX and Linux client systems.

Using NFS, a local system can mount and use a disk partition or a file system from a remote system (an NFS server), as if it were local. The Veritas Access NFS server exports a directory, with selected permissions and options, and makes it available to NFS clients.

The selected permissions and options can also be updated, by adding or removing permissions, to restrict or expand the permitted use.

The Veritas Access NFS service is clustered. The NFS clients continuously retry during a failover transition. Even if the TCP connection is broken for a short time, the failover is transparent to NFS clients, and NFS clients regain access transparently as soon as the failover is complete.

See [“About using NFS server with Veritas Access”](#) on page 141.

## Displaying file systems and snapshots that can be exported

### To display a file system and snapshots that can be exported

- ◆ To display online file systems and the snapshots that can be exported, enter the following:

```
NFS> show fs
```

For example:

```
NFS> show fs
FS/Snapshot
=====
fs1
```

## Exporting an NFS share

You can export an NFS share with the specified NFS options that can then be accessed by one or more client systems.

If you add a directory that has already been exported with a different NFS option (rw, ro, async, or secure, for example), Veritas Access provides a warning message saying that the directory has already been exported. Veritas Access updates (overwrite) the old NFS options with the new NFS options.

Directory options appear in parentheses.

If a client was not specified when the `NFS> share add` command was used, then `*` is displayed as the system to be exported to, indicating that all clients can access the directory.

Directories that have been exported to multiple clients appear as separate entries. Directories that are exported to <world> and other specific clients also appear as separate entries.

For example:

Consider the following set of exported directories where only the client (1.1.1.1) has **read-write** access to directory (fs2), while all other clients have **read** access only.

```
/vx/fs2          * (ro)
/vx/fs2 1.1.1.1 (rw)
```

Exporting the same directory to multiple clients with different permissions is not supported with NFS-Ganesha.

When sharing a directory, Veritas Access does not check whether the client exists or not. If you add a share for an unknown client, then an entry appears in the `NFS> show` command output.

The `NFS> show fs` command displays the list of exportable file systems. If a directory does not exist, the directory is automatically created and exported when you try to export it.

Valid NFS options include the following:

<code>rw</code>	Grants read and write permission to the directory (including all files under the directory that reside on the exported directory's file system). Hosts mounting this directory will be able to make changes to the directory.
<code>ro (Default)</code>	Grants read-only permission to the directory. Hosts mounting this directory will not be able to change it.
<code>sync (Default)</code>	Grants synchronous write access to the directory. Forces the server to perform a disk write before the request is considered complete.
<code>async</code>	Grants asynchronous write access to the directory. Allows the server to write data to the disk when appropriate.
<code>secure (Default)</code>	Grants secure access to the directory. Requires that clients originate from a secure port. A secure port is between 1-1024.
<code>insecure</code>	Grants insecure access to the directory. Permits client requests to originate from unprivileged ports (those above 1024).
<code>secure_locks (Default)</code>	Requires authorization of all locking requests. This option is not supported with NFS-Ganesha.

<code>insecure_locks</code>	<p>Some NFS clients do not send credentials with lock requests, and therefore work incorrectly with <code>secure_locks</code>, in which case you can only lock world-readable files. If you have such clients, either replace them with better ones, or use the <code>insecure_locks</code> option. This option is not supported with NFS-Ganesha.</p>
<code>root_squash</code> (Default)	<p>Prevents the root user on an NFS client from having root privileges on an NFS mount.</p> <p>This effectively "squashes" the power of the remote root user to the lowest local user, preventing remote root users from acting as though they were the root user on the local system.</p>
<code>no_root_squash</code>	<p>Disables the <code>root_squash</code> option. Allows root users on the NFS client to have root privileges on the NFS server.</p>
<code>wdelay</code> (Default)	<p>Causes the NFS server to delay writing to the disk if another write request is imminent. This can improve performance by reducing the number of times the disk must be accessed by separate write commands, reducing write overhead.</p> <p><b>Note:</b> The <code>wdelay</code> option is deprecated, and is supported for backward-compatibility only.</p> <p>This option is not supported with NFS-Ganesha.</p>
<code>no_wdelay</code>	<p>Disables the <code>wdelay</code> option.</p> <p>The <code>no_wdelay</code> option has no effect if the <code>async</code> option is also set.</p> <p><b>Note:</b> The <code>no_wdelay</code> option is deprecated, and is supported for backward-compatibility only. Using the <code>no_wdelay</code> option is always effective.</p> <p>This option is not supported with NFS-Ganesha.</p>
<code>subtree_check</code>	<p>Verifies that the requested file is in an exported subdirectory. If this option is turned off, the only verification is that the file is in an exported file system. This option is not supported with NFS-Ganesha.</p>
<code>no_subtree_check</code> (Default)	<p>Sometimes subtree checking can produce problems when a requested file is renamed while the client has the file open. If many such situations are anticipated, it might be better to set <code>no_subtree_check</code>. One such situation might be the export of the home directory. Most other situations are best handled with <code>subtree_check</code>. This option is not supported with NFS-Ganesha.</p>

<code>fsid</code> (Default)	Allows the Veritas Access administrator to associate a specific number as <code>fsid</code> with the share. This option is not supported with NFS-Ganesha.
<code>nordirplus</code>	Allows you to disable a <code>readdirplus</code> remote procedure call (RPC).
<code>sec</code>	Specifies the Kerberos security options for exporting an NFS share. The value can be <code>krb5</code> , <code>krb5i</code> , <code>krb5p</code> , or <code>sys</code> . The <code>sys</code> option does not provide Kerberos authentication. The other options use Kerberos V5 to authenticate users to the NFS server.  See <a href="#">“Exporting an NFS share for Kerberos authentication”</a> on page 410.

For example, you could issue the following commands:

```
NFS> share add rw,async /vx/fs2  
  
NFS> share add rw,sync,secure,root_squash /vx/fs3 10.10.10.10  
  
NFS> share add rw,sync,no_root_squash /vx/fs3 2001:21::/120  
Exporting /vx/fs3 with options rw,sync,no_root_squash  
Success.
```

---

**Note:** With `root_squash`, the root user can access the share, but with 'nobody' permissions.

---

**To export a directory/file system**

- 1** To see your exportable online file systems and snapshots, enter the following:

```
NFS> show fs
```

For example:

```
NFS> show fs
FS/Snapshot
=====
fs2
fs3
```

- 2** To see your NFS shares and their options, enter the following:

```
NFS> share show
```

For example:

```
NFS> share show
/vx/fs2          * (sync)
/vx/fs3          * (secure,ro,no_root_squash)

NFS> share show
/vx/fs3          2001:21::/120 (rw,sync,no_root_squash)
```

- 3** To export a directory, enter the following command:

```
NFS> share add nfsoptions export_dir [client]
```

*nfsoptions*            Comma-separated list of export options from the set.

*export\_dir*            Specifies the name of the directory you want to export.

The directory name should start with */vx*, and only *a-zA-Z0-9\_/@+.=.-* characters are allowed for *export\_dir*.

client

Clients may be specified in the following ways:

- Single host - specify a host either by an abbreviated name that is recognized by the resolver (DNS is the resolver), the fully qualified domain name, or an IP address.
- Netgroups - specify netgroups as *@group*. Only the host part of each netgroup member is considered for checking membership.
- IP networks - specify an IP address and netmask pair (address/netmask) to simultaneously export directories to all hosts on an IP sub-network. Specify the netmask as a contiguous mask length. You can specify either an IPv4 address or an IPv6 address.

If the client is not given, then the specified directory can be mounted or accessed by any client. To re-export new options to an existing share, the new options will be updated after the command is run.

Example using NFS options:

```
NFS> share add async /vx/fs1
Exporting */vx/fs1 with options async
..Success.
```

## Exporting an NFS share for Kerberos authentication

Kerberos provides three types of security options for exporting an NFS share:

- `krb5`
- `krb5i`
- `krb5p`

Veritas Access also provides a `sys` (`sec=sys`) export option, which does not provide Kerberos authentication. Veritas Access supports all of the three types of Kerberos security options. All of the security options use Kerberos V5 to authenticate users to NFS servers.

`krb5i` computes a hash on every remote procedure (RPC) call request to the server and every response to the client. The hash is computed on an entire message: RPC header, plus NFS arguments or results. Since the hash information travels with the NFS packet, any attacker modifying the data in the packet can be detected. Thus `krb5i` provides integrity protection.

`krb5p` uses encryption to provide privacy. With `krb5p`, NFS arguments and results are encrypted, so a malicious attacker cannot spoof on the NFS packets and see file data or metadata.

---

**Note:** Since `krb5i` and `krb5p` perform an additional set of computations on each NFS packet, NFS performance decreases as compared with `krb5`.

---

Performance decreases in the following order: `krb5` > `krb5i` > `krb5p`.

`krb5` provides better performance and `krb5p` gives the least performance.

Additional export options are available.

See “[Exporting an NFS share](#)” on page 405.

**To export a directory using only the `krb5` mount option**

- ◆ Export a directory using only the `krb5` mount option:

```
NFS> share add sec=krb5 /vx/fs1
Exporting /vx/fs1 with options sec=krb5
Success.
```

**To export a directory using `krb5`, `krb5i`, `krb5p`, and `sys` options**

- ◆ Export a directory using `krb5`, `krb5i`, `krb5p`, and `sys` options.

```
NFS> share add sec=krb5:krb5i:krb5p:sys /vx/fs1
Exporting /vx/fs1 with options sec=krb5:krb5i:krb5p:sys
Success.
```

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, it is `krb5p`.

## Mounting an NFS share from the NFS client

This section explains how the NFS client will NFS mount with the Kerberos mount options. This procedure assumes that the NFS service principal of the NFS client is added to the KDC server, and the keytab is copied at the appropriate location on the client.

The steps may differ depending on the operating system and version of the client. On a Red Hat Enterprise Linux (RHEL) client, Kerberos can be configured as follows.

### To mount the NFS client with the Kerberos mount options

- 1 Create the NFS service principal for the client on the KDC server and copy it to the client system at `/etc/krb5.keytab`.
- 2 Configure the `/etc/krb5.conf` file with the KDC details.
- 3 Enable `SECURE_NFS=yes` in the `/etc/sysconfig/nfs` file.
- 4 Start the `rpcgssd` service.

```
# service rpcgssd start
```

- 5 Keep the clocks of the KDC server, the Veritas Access server, and the NFS client in sync.

A maximum of a five-minute variation is accepted, or otherwise the Kerberos NFS mount fails.

```
[root@krb-client]# mount -o vers=4,sec=krb5 10.209.107.24:/vx/fs2/share1 /mnt/share1
```

Make sure that the virtual IP that is used for mounting can use reverse name lookup to the Veritas Access cluster name. For example, if `access_ga` is the cluster name, then in the above example, `access_ga` should look up to 10.209.107.24 and vice versa. If the IP 10.209.107.24 can be looked up by multiple host names, make sure that the entry `access_ga` is first in the reverse lookup.

- 6 Make sure the users accessing the NFS share are already added on the KDC server.

Use `kinit` to get the ticket granting ticket from the KDC server on the NFS client.

```
[root@krb-client]# su - sfuuser2

[sfuuser2@krb-client ~]$ kinit
Password for sfuuser2@TESTKDC.COM:
[sfuuser2@krb-client ~]$ cd /mnt/share1
[sfuuser2@krb-client share1]$ touch test.txt
[sfuuser2@krb-client share1]$
[sfuuser2@krb-client share1]$ ls -al total 4
drwxrwxrwx 2 root root 96 May 14 16:03 .
drwxr-xr-x 17 root root 4096 May 7 19:41 ..
-rw-r--r-- 1 sfuuser2 sfugroup1 0 May 14 16:03 test.txt
```

# Displaying exported directories

You can display the exported directories and the NFS options that are specified when the directory was exported. For NFS-Ganesha (GNFS), the output also shows the virtual IP address that must be used on the client to mount the GNFS shares for the shares that are exported from scale-out file systems.

## To display exported directories

To display exported directories, enter the following:

```
NFS> share show
```

For example, for the kernel NFS server:

```
NFS> share show
/vx/fs2          * (sync)
/vx/fs3          * (secure,ro,no_root_squash)
```

The command output displays the following columns:

**Left-hand column** Displays the directory that was exported.

For example:

```
/vx/fs2
```

**Right-hand column** Displays the system that the directory is exported to, and the NFS options with which the directory was exported.

For example:

```
* (secure,ro,no_root_squash)
```

For example, for the NFS-Ganesha server:

```
NFS> share show
/vx/fs1          * (rw,async) 10.209.106.180
```

The command output displays the following columns:

**Left-hand column** Displays the directory that was exported.

For example:

```
/vx/fs1
```

Middle column	<p>Displays the system that the directory is exported to, and the NFS options with which the directory was exported.</p> <p>For example:</p> <pre>* (rw,async)</pre>
Right-hand column	<p>Displays the virtual IP address that must be used on the client to mount the GNFS shares of scale-out file systems.</p> <p>For example:</p> <p>Use the address <code>10.209.106.180</code> to mount the <code>/vx/fs1</code> file system.</p>

## About managing NFS shares using netgroups

A netgroup defines a network-wide group of hosts and users. You use netgroups for restricting access to shared NFS file systems and to restrict remote login and shell access.

Each line in the netgroup file consists of a netgroup name followed by a list of members, where a member is either another netgroup name, or a comma-separated list of host, user, or a domain. Host, user, and domain are character strings for the corresponding components. Any of these three fields can be empty, which indicates a wildcard, or may consist of the string "-" to indicate that there is no valid value for the field. 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 any security. The domain field refers to the domain in which the host is valid, not the domain containing the trusted host.

When exporting a directory by NFS with the specified options, clients may be specified using netgroups. Netgroups are 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
```

## Configuring netgroups

When you add data to an existing netgroup, the new data cannot be the same as the existing data of that netgroup. That is, you cannot add the same member to the netgroup more than once. If the netgroup does not exist, create a new netgroup. You can delete the members of an existing netgroup. If you delete a netgroup without a member list, you delete that netgroup.

Additional configuration is necessary for netgroups using the `Network> nsswitch` commands.

See [“Configuring NSS lookup order”](#) on page 83.

## To add, delete, or display a netgroup

### 1 Create a new netgroup or add members to an existing netgroup.

```
Network> netgroup add groupname memberlist
```

*groupname* Netgroup name.

*memberlist* Comma-separated member list. A member can be an IP version 4 address, an IP version 6 address, a netgroup name, or a hostname.

**Note:** It is recommended that you use the fully qualified domain name of the host rather than an IP address. If a fully qualified domain name is not available, an IP version 4 address or an IP version 6 address also works.

The hostname can include the characters a-z | A-Z | 0-9 or a hyphen (-). Each level of the hostname should be between 1 and 63 characters long and should not start or end with a hyphen (-). The last TLD (Top Level Directory) must be at least two characters and a maximum of six characters.

For example:

```
Network> netgroup add group1 10.200.114.173,cdc.example.com,2002:4559:1fe2:0:0:0:4559:1f,vip  
ACCESS Netgroup SUCCESS V-288-1397 Netgroup group1 created.
```

### 2 Delete the members of an existing netgroup or delete the entire netgroup.

```
Network> netgroup delete groupname memberlist
```

For example:

```
Network> netgroup delete dev 192.168.0.1,www.sina.com  
ACCESS Netgroup SUCCESS V-288-1397 Members 192.168.0.1,www.sina.com of netgroup dev has  
been deleted.
```

### 3 Display the netgroup.

```
Network> netgroup show
```

For example:

```
Network> netgroup show wto
Netgroup Name      Member List
-----
wto                 china.org,us.com,vip,192.168.0.50,2002:4559:1fe2:0:0:0:45:88
```

## Exporting an NFS snapshot

### To export an NFS snapshot

#### 1 For example, to create an NFS snapshot, enter the following:

```
Storage> snapshot create fs5sp1 FS5
```

See [“About snapshots”](#) on page 574.

#### 2 For example, to export the NFS snapshot, enter the following:

```
NFS> share add rw /vx/FS5:fs5sp1
```

See [“Exporting an NFS share ”](#) on page 405.

## Unexporting a directory or deleting NFS options

You can unexport the share of the exported directory.

---

**Note:** You will receive an error message if you try to remove a directory that does not exist.

---

## To unexport a directory or delete NFS options

- 1 To see your existing exported resources, enter the following command:

```
NFS> share show
```

Only the directories that are displayed can be unexported.

For example:

```
NFS> share show
/vx/fs2          * (sync)
/vx/fs3          * (secure,ro,no_root_squash)
```

- 2 To delete a directory from the export path, enter the following command:

```
NFS> share delete export_dir [client]
```

For example:

```
NFS> share delete /vx/fs3
Removing export path */vx/fs3
..Success.
```

**export\_dir** Specifies the name of the directory you want to delete. The directory name should start with `/vx`, and only `a-zA-Z0-9_/@+.= :-` characters are allowed in `export_dir`. You cannot include single or double quotes that do not enclose characters.

```
NFS> share delete "*/vx/example"
```

client

Clients may be specified in the following ways:

- Single host - specify a host either by an abbreviated name that is recognized by the resolver (DNS is the resolver), the fully qualified domain name, or an IP address.
- Netgroups - specify netgroups as @group. Only the host part of each netgroup member is considered for checking membership.
- IP networks - specify an IP address and netmask pair (address/netmask) to simultaneously export directories to all hosts on an IP sub-network. Specify the netmask as a contiguous mask length.

If *client* is included, the directory is removed from the export path that was directed at the *client*.

If a directory is being exported to a specific client, the `NFS> share delete` command must specify the client to remove that export path.

If the client is not specified, then the specified directory can be mounted or accessed by any client.

# Creating and maintaining CIFS shares

This chapter includes the following topics:

- [About managing CIFS shares](#)
- [Exporting a directory as a CIFS share](#)
- [Configuring a CIFS share as secondary storage for an Enterprise Vault store](#)
- [Exporting the same file system/directory as a different CIFS share](#)
- [About the CIFS export options](#)
- [Setting share properties](#)
- [Hiding system files when adding a CIFS normal share](#)
- [Displaying CIFS share properties](#)
- [Allowing specified users and groups access to the CIFS share](#)
- [Denying specified users and groups access to the CIFS share](#)
- [Exporting a CIFS snapshot](#)
- [Deleting a CIFS share](#)
- [Modifying a CIFS share](#)
- [Making a CIFS share shadow copy aware](#)

## About managing CIFS shares

You can export the Veritas Access file systems to clients as CIFS shares. When a share is created, it is given a name. The share name is different from the file system name. Clients use the share name when they import the share.

---

**Note:** You cannot export a scale-out file system as a CIFS share.

---

You create and export a share with one command. The same command binds the share to a file system, and you can also use it to specify share properties.

In addition to exporting file systems as CIFS shares, you can use Veritas Access to store user home directories. Each of these home directories is called a home directory share. Shares that are used to export ordinary file systems (that is, file systems that are not used for home directories), are called ordinary shares to distinguish them from home directory shares.

## Exporting a directory as a CIFS share

Directory-level share support is available only in the ctdb clustering mode. If you want to export a directory as a CIFS share, you must first switch to the ctdb clustering mode.

See [“About CIFS clustering modes”](#) on page 210.

See [“Switching from normal to ctdb clustering mode”](#) on page 212.

**To check the status of the CIFS server to confirm that the clustering mode is set to ctdb**

- ◆ To check the status of the CIFS server to confirm that the clustering mode is set to ctdb, enter the following:

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

Homedirfs           : fs1
Security            : ads
Domain membership status : Enabled
Domain              : VERITASDOMAIN.COM
Workgroup           : VERITASDOMAIN
Domain Controller   : VRTSSERVER
Domain User         : administrator
Clustering Mode     : ctdb
```

**Configuring a CIFS share as secondary storage for an Enterprise Vault store****To export a directory as a CIFS share**

- 1 To export a directory as a CIFS share, enter the following:

```
CIFS> share add fs1/access share1 rw,full_acl
Exporting CIFS filesystem : share1 ..Success.
```

If the directory name contains a space, enter the directory name with double quotes (" "). For example:

```
CIFS> share add "fs1/Veritas access" share2 rw
Exporting CIFS filesystem : share2 ..Success.
```

- 2 To list the CIFS shares, enter the following:

```
CIFS> share show
ShareName FileSystem      ShareOptions
share2     fs1/access  owner=root,group=root,fs_mode=755,rw
share1     fs1/access  owner=root,group=root,fs_mode=755,rw,full_acl
```

## Configuring a CIFS share as secondary storage for an Enterprise Vault store

You can use Veritas Access as secondary storage with Enterprise Vault 12.0 by exporting the file system over the CIFS protocol.

---

**Note:** Before configuring the CIFS share path as secondary storage, you need to verify that the CIFS share path is accessible. Confirm that I/O operations can occur on the CIFS share.

---

### Configuring a CIFS share as secondary storage for an Enterprise Vault store

- 1 On the Veritas Access cluster, you export the file system over the CIFS protocol using the following CIFS export options: `fs_mode=1777,rw,full_acl`.  
See [“About the CIFS export options”](#) on page 424.
- 2 On the Enterprise Vault server, open the Enterprise Vault console.
- 3 Right-click on the partition that is created on **Vault Store > Properties**.  
Enterprise Vault brings up the **Vault Store Partition Properties** window.
- 4 In the **Vault Store Partition Properties** window, select the **Migration** tab.

- 5 Specify the path of the CIFS share in the **Secondary storage location** text box.

Example:

*\\IP address of the CIFS share\name of file system*

- 6 Press **Apply**.

## Exporting the same file system/directory as a different CIFS share

In ctdb clustering mode, you can export the same file system or directory as a different CIFS share with different available CIFS options. This feature allows you more granular control over CIFS shares for different sets of users.

If the same file system is exported as different shares in ctdb clustering mode, then after switching to normal clustering mode only one share out of these is available.

---

**Note:** If the same file system or directory is exported as different shares, then the `fs_mode` value is the same for all of these shares; that is, the last modified `fs_mode` value is applicable for all of those shares.

---



---

**Note:** This feature is only supported in the ctdb clustering mode.

---

**To export a directory with read access to everyone, but write access to the limited set of users who need to be authenticated**

- ◆ To export a directory with read access to everyone, but write access to the limited set of users who need to be authenticated, enter the following:

```
CIFS> share add "fs1/Veritas isa" share1 rw,noguest
Exporting CIFS filesystem : share1 ..Success.

CIFS> share add "fs1/Veritas isa" share2 ro,guest
Exporting CIFS filesystem : share21 ..Success.

CIFS> share show
ShareName FileSystem      ShareOptions
share1     fs1/access  owner=root,group=root,fs_mode=755,rw,noguest
share2     fs1/access  owner=root,group=root,fs_mode=755,ro,guest
```

The above example illustrates that the same directory is exported as a different CIFS share for `guest` and `noguest` users with different sets of permissions.

## About the CIFS export options

The following are the CIFS export options.

**Table 24-1** CIFS export options

CIFS export option	Definition
rw	There is a share option which specifies if the files in the share will be read-only or if both read and write access will be possible, subject to the authentication and authorization checks when a specific access is attempted. This share option can be given one of these values, either <code>rw</code> or <code>ro</code> .  Grants read and write permission to the exported share.
ro (Default)	Grants read-only permission to the exported share. Files cannot be created or modified.

**Table 24-1** CIFS export options (*continued*)

CIFS export option	Definition
guest	<p>Another configuration option specifies if a user trying to establish a CIFS connection with the share must always provide the user name and password, or if they can connect without it. In this case, only restricted access to the share will be allowed. The same kind of access is allowed to <code>anonymous</code> or <code>guest</code> user accounts. This share option can have one of the following values, either <code>guest</code> or <code>noguest</code>.</p> <p>Veritas Access allows restricted access to the share when no user name or password is provided.</p>
noguest (Default)	<p>Veritas Access always requires the user name and password for all of the connections to this share.</p>
full_acl	<p>All Windows Access Control Lists (ACLs) are supported except in the case when you attempt using the Windows Explorer folder <b>Properties &gt; Security GUI</b> to inherit down to a non-empty directory hierarchy while denying all access to yourself.</p>
no_full_acl (Default)	<p>Some advanced Windows Access Control Lists (ACLs) functionality does not work. For example, if you try to create ACL rules on files saved in a CIFS share using Windows explorer while allowing some set of file access for <code>user1</code> and denying file access for <code>user2</code>, this is not possible when CIFS shares are exported using <code>no_full_acl</code>.</p>
hide_unreadable	<p>Prevents clients from seeing the existence of files and directories that are not readable to them.</p> <p>The default is: <code>hide_unreadable</code> is set to off.</p>
veto_sys_files	<p>To hide some system files (lost+found, quotas, quotas.grp) from displaying when using a CIFS normal share, you can use the <code>veto_sys_files</code> CIFS export option. For example, when adding a CIFS normal share, the default is to display the system files. To hide the system files, you must use the <code>veto_sys_files</code> CIFS export option.</p>
fs_mode	<p>When a file system or directory is exported by CIFS, its mode is set to an <code>fs_mode</code> value. It is the UNIX access control set on a file system, and CIFS options like <code>rw/ro</code> do not take precedence over it. This value is reset to <code>0755</code> when the CIFS share is deleted.</p> <p>The default is: <code>fs_mode = 1777</code>.</p>

**Table 24-1** CIFS export options (*continued*)

CIFS export option	Definition
dir_mask	<p>When a directory is created under a file system or directory exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permissions. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a directory when it is created.</p> <p>The default is: <code>dir_mask = 0775</code>.</p>
create_mask	<p>When a file is created under a file system or directory exported by CIFS, the necessary permissions are calculated by mapping DOS modes to UNIX permissions. The resulting UNIX mode is then bit-wise 'AND'ed with this parameter. Any bit not set here is removed from the modes set on a file when it is created.</p> <p>The default is: <code>create_mask = 0775</code>.</p>
oplocks (Default)	<p>Veritas Access supports the CIFS opportunistic locks. You can enable or disable them for a specific share. The opportunistic locks improve performance for some workloads, and there is a share configuration option which can be given one of the following values, either oplocks or nooplocks.</p> <p>Veritas Access supports opportunistic locks on the files in this share.</p>
nooplocks	<p>No opportunistic locks will be used for this share.</p> <p>Disable the oplocks when:</p> <ul style="list-style-type: none"> <li>■ 1) A file system is exported over both CIFS and NFS protocols.</li> <li>■ 2) Either CIFS or NFS protocol has read and write access.</li> </ul>
owner	<p>There are more share configuration options that can be used to specify the user and group who own the share. If you do not specify these options for a share, Veritas Access uses the current values as default values for these options. You may want to change the default values to allow a specific user or group to be the share owner.</p> <p>Irrespective of who are owner and group of the exported share, any CIFS clients can create folders and files in the share. However, there are some operations that require owner privileges; for example, changing the owner itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the owner option to a specific user name, and this user can perform the privileged operations.</p>

**Table 24-1** CIFS export options (*continued*)

CIFS export option	Definition
group	<p>By default, the current group is the primary group owner of the root directory of the exported share. This lets CIFS clients create folders and files in the share. However, there are some operations that require group privileges; for example, changing the group itself, and changing permissions of the top-level folder (that is, the root directory in UNIX terms). To enable these operations, you can set the <code>group</code> option to a specific group name, and this group can perform the privileged operations.</p>
ip	<p>Veritas Access lets you specify a virtual IP address. If you set <code>ip=virtualip</code>, the share is located on the specified virtual IP address. This address must be part of the Veritas Access cluster, and is used by the system to serve the share internally.</p> <p><b>Note:</b> <code>ip</code> is not a valid CIFS option when using the <code>ctdb</code> clustering mode.</p> <p>See <a href="#">“About CIFS clustering modes”</a> on page 210.</p>
max_connections	<p>Specify the maximum limit for concurrent CIFS connections for a CIFS share.</p> <p>The default value is 0, indicating that there are no limited connections.</p>
shadow_copy	<p>Indicates that this is a <code>shadow_copy</code> capable CIFS share.</p> <p>See <a href="#">“Making a CIFS share shadow copy aware”</a> on page 436.</p>
enable_encryption	<p>If <code>enable_encryption</code> is set, then all the traffic to a share must be encrypted once the connection has been made to the share. The server will return an <code>access denied</code> message to all unencrypted requests on such a share. As SMB3 is the max protocol, only SMB3 clients supporting encryption will be able to connect to the share.</p>
disable_encryption	<p>If <code>disable_encryption</code> is set, then encryption cannot be negotiated by the client. SMB1, SMB2, and SMB3 clients can connect to the share.</p>
enable_durable_handles	<p>Enables support for durable handles for CIFS shares. Enabling this option disables use of POSIX/fcntl locks. Exporting the same CIFS share using NFS may result in data corruption. For support for durable handles on CIFS shares, you must specify this option.</p>

# Setting share properties

After a file system is exported as a CIFS share, you can change one or more share options. This is done using the same `share add` command, giving the name of an existing share and the name of the file system exported with this share. Veritas Access will realize the given share has already been exported and that it is only required to change the values of the share options.

For example, to export the file system `fs1` with the name `share1`, enter the following:

```
CIFS> share add fs1 share1 "owner=administrator,group=domain users,rw"
Exporting CIFS filesystem : share1 ...
CIFS> share show
ShareName      FileSystem    ShareOptions
share1         fs1          owner=administrator,group=domain
users,rw
```

## To export a file system

- ◆ Export a file system, enter the following:

```
CIFS> share add filesystem sharename \
[@virtual_ip] [cifsoptions]
```

filesystem	A Veritas Access file system that you want to export as a CIFS share. The given file system must not be currently used for storing the home directory shares.  The file system or directory path should always start with the file system name, not with the file system mount point <code>/vx</code> .
sharename	The name for the newly-exported share. Names of the Veritas Access shares can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "_" and "-". ("-" cannot be used as the first character in a share name).  <b>Note:</b> A share name cannot exceed 256 characters.

**@virtual\_ip** Specifies an optional full identifier allowing a virtual IP to access the specified CIFS share.

Veritas Access provides unified access to all shares through virtual IPs.

If a CIFS share is added with the `@virtual_ip` full identifier, the CIFS share is created by allowing only this virtual IP to access this CIFS share.

```
CIFS> share show
ShareName FileSystem ShareOptions
share1@10.200.60.105 fs1 owner=root,group=root,
fs_mode=1777,rw
share1@10.200.60.106 fs2 owner=root,group=root,
fs_mode=1777,rw
```

**cifsoptions** A comma-separated list of CIFS export options. This part of the command is optional.

If a CIFS export option is not provided, Veritas Access uses the default value.

See [“About the CIFS export options”](#) on page 424.

For example, an existing file system called `FSA` being exported as a share called `ABC`:

```
CIFS> share add FSA ABC rw,guest,owner=john,group=abcdev
```

## Hiding system files when adding a CIFS normal share

When adding a CIFS normal share, the default is to display the system files (`lost+found`, `quotas`, `quotas.grp`). To hide the system files, you must use the `veto_sys_files` CIFS export option.

See [“About the CIFS export options”](#) on page 424.

**To hide system files when adding a CIFS normal share**

- ◆ To hide system files when adding a CIFS normal share, enter the following:

```
CIFS> share add filesystem sharename [cifsoption]
```

Use the `veto_sys_files` CIFS export option to hide system files.

For example:

```
CIFS> share add fs1 share1 veto_sys_files
Exporting CIFS filesystem : share1 ...Success.
CIFS> share show
ShareName FileSystem ShareOptions
share1 fs1 owner=root,group=root,fs_mode=1777,veto_sys_files

CIFS> share show
ShareName FileSystem ShareOptions
share2 fs2 owner=root,group=root,fs_mode=1777
.....Done

CIFS> share show
ShareName FileSystem ShareOptions
share2 fs2 owner=root,group=root,fs_mode=1777,veto_sys_files
```

# Displaying CIFS share properties

## To display share properties

- 1 To display the information about all of the exported shares, enter the following:

```
CIFS> share show
```

For example:

```
CIFS> share show
```

ShareName	FileSystem	ShareOptions
cifs1	fs1	owner=root,group=root,fs_mode=1777,rw
cifs2	fs2	owner=root,group=root,fs_mode=1777,oplocks,ro,full_acl
cifs3	fs3	owner=root,group=root,fs_mode=1777,veto_sys_files,no_full_acl

- 2 To display the information about one specific share, enter the following:

```
CIFS> share show sharename
```

For example:

```
CIFS> share show share1
```

ShareName	VIP Address
cifs1	10.10.10.10

# Allowing specified users and groups access to the CIFS share

## To allow specified users and groups access to the CIFS share

- ◆ To allow specified users and groups access to the CIFS share, enter the following:

```
CIFS> share allow sharename @group1 \  
[,@group2,user1,user2,...]
```

sharename	<p>Name of the CIFS share for which you want to allow specified users and groups access.</p> <p>Names of the Veritas Access shares are non case sensitive and can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "_" and "-". ("-", cannot be used as the first character in a share name).</p>
group	<p>If the CIFS server joined a domain, and there is a space in the user or group name, the user or group name needs to be entered with double quotes (for example, "@domain users").</p> <p>By default, all groups are allowed to access the shares.</p> <p>In the case where a CIFS share has joined a domain, and the domain contains trusted domains, and <code>allow_trusted_domains</code> is set to <code>yes</code> on the CIFS server, if you want to allow/deny users or groups from the trusted domains, the user or group needs to be prefixed with the trusted domain name. Separate the domain and user/group with a double backslash.</p> <p>For example:</p> <pre>CIFS&gt; share allow sharename "@domain name\\group name"</pre>
user	<p>Name of the CIFS user allowed access to the CIFS share.</p> <p>By default, all users are allowed to access the shares.</p> <p>If <code>all</code> is specified, then default access restrictions are restored on the CIFS share.</p> <pre>CIFS&gt; <b>share allow share1 user1,@group1</b> Warning: Modifying an already existing share. .....Done</pre>

# Denying specified users and groups access to the CIFS share

## To deny specified users and groups access to the CIFS share

- ◆ To deny specified users and groups access to the CIFS share, enter the following:

```
CIFS> share deny sharename \  

    @group1[,@group2,user1,user2,...]
```

*sharename* Name of the CIFS share for which you want to deny specified users and groups access.

Names of the Veritas Access shares are non case sensitive and can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "\_" and "-". ("-", cannot be used as the first character in a share name).

*group* If the CIFS server joined a domain, and there is a space in the user or group name, the user or group name needs to be entered with double quotes (for example, "@domain users").

By default, all groups are allowed to access the shares.

In the case where a CIFS share has joined a domain, and the domain contains trusted domains, and CIFS is set to trusted domains as true, if you want to allow/deny users or groups from the trusted domains, the user or group needs to be prefixed with the trusted domain name. Separate the domain and user/group with a double backslash.

For example:

```
CIFS> share deny sharename  

"@domain name\\user name"
```

*user* Name of the CIFS user denied access to the CIFS share.

By default, all users are allowed to access the shares.

If *all* is specified, then all the users and groups are not able to access the share.

```
CIFS> share deny share1 user1,@group1  

Warning: Modifying an already existing share.  

.....Done
```

## Exporting a CIFS snapshot

### To export a CIFS snapshot

- 1 To create a CIFS snapshot, enter the following for example:

```
Storage> snapshot create cf11sp1 CF11
```

See “[About snapshots](#)” on page 574.

- 2 To export the CIFS snapshot, enter the following for example:

```
CIFS> share add CF11:cf11sp1 cf11sp1 rw,guest
```

A client can access the CIFS snapshot by the CIFS share name, `cf11sp1`.

## Deleting a CIFS share

### To delete a CIFS share

- 1 To delete a share, enter the following:

```
CIFS> share delete sharename [@virtual_ip]
```

*sharename* Specifies the name of the share that you want to delete.

*@virtual\_ip* Specifies an optional full identifier allowing a virtual IP to access the specified CIFS share.

For example:

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

- 2 To confirm the share is no longer exported, enter the following:

```
CIFS> share show  
ShareName   FileSystem  ShareOptions  
share2      fs2         owner=root,group=root
```

In the case of any remanent sessions (sessions that are not closed while deleting a CIFS share), Veritas Access displays the following output:

```
CIFS> share delete share2  
Unexporting CIFS share : share2 ....Success.  
ACCESS cifs WARNING V-288-0 There are following remanent sessions.  
Clients may still access 'share4' unless the relevant processes are
```

```
killed.  
  
Remanent Sessions  
pid      nodename  
-----  
13966    accessnode_01  
14130    accessnode_02
```

This is a rare situation, and it occurs if the following conditions are met:

- CIFS server is online
- CIFS share that is being deleted is ONLINE
- There are some existing client connections with that CIFS share
- While deleting the share, some remanent sessions are left

If any condition is failed above, then the `CIFS> share delete` command output displays as usual.

```
CIFS> share delete share2  
Unexporting CIFS share : share2 ....Success.
```

## Modifying a CIFS share

You can re-export the file system with the given share name. The new options are updated after the command is run.

### To modify a CIFS share

- ◆ To modify a CIFS share, enter the following:

```
CIFS> share modify sharename[@virtual_ip] [cifsoptions]
```

sharename	The name of the CIFS share that you want to modify.  Names of the Veritas Access shares can consist of the following characters: lower and uppercase letters "a" - "z" and "A" - "Z," numbers "0" - "9" and special characters: "_" and "-". ("-" cannot be used as the first character in a share name).
@virtual_ip	Specifies an optional full identifier allowing a virtual IP to access the specified CIFS share.  Veritas Access provides unified access to all shares through virtual IPs.
cifsoptions	A comma-separated list of CIFS export options.  If a CIFS export option is not provided, Veritas Access uses the default value.  See <a href="#">"About the CIFS export options"</a> on page 424.

For example:

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

CIFS> share show
ShareName FileSystem ShareOptions
share2 fsl/dir2 a owner=root,group=root,fs_mode=1777,ro,full_acl
share1 fsl/dir1 owner=root,group=root,fs_mode=755,rw,full_acl
```

## Making a CIFS share shadow copy aware

Shadow Copy (Volume Snapshot Service or Volume Shadow Copy Service or VSS) is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of data on a specific volume at a specific point in time over regular intervals.

### To make a CIFS share shadow copy aware

- ◆ Add the CIFS export option `shadow_copy` to the CIFS share.

For example:

```
CIFS> share add fs1 share1 rw,shadow_copy
```

```
CIFS> share show share1
```

ShareName	FileSystem	ShareOptions
share1	fs1	rw,shadow_copy

See [“About the CIFS export options”](#) on page 424.

# Creating and maintaining S3 shares

This chapter includes the following topics:

- [Managing the Veritas Access S3 share](#)

## Managing the Veritas Access S3 share

You can export any file system as an S3 share. See the `objectaccess` man page for more information.

- Export a file system as an S3 share:

```
ObjectAccess> share add S3 export_dir
```

```
CLUSTERNAME.ObjectAccess> share add S3 /vx/ForWin  
ACCESS ObjectAccess SUCCESS V-288-0 Exporting /vx/ForWin as an S3 share
```

- Display all the shared file systems that are available for S3:

```
ObjectAccess> share show
```

```
Name                               Type  
=====                           =====  
/vx/File_System_RC2                S3  
/vx/ForS3                           S3  
/vx/ForWin                          S3  
/vx/Multiprotocol                   S3
```

- Remove a share from S3 shares:

```
ObjectAccess> share delete export_dir
```

```
CLUSTERNAME.ObjectAccess> share delete /vx/ForWin  
ACCESS ObjectAccess SUCCESS V-288-0 Removing /vx/ForWin as an S3 share
```

You should delete the associated account before you delete the share, otherwise you get an error:

```
CLUSTER_NAME> objectaccess share delete /vx/Multiprotocol  
ACCESS ObjectAccess ERROR V-288-0 /vx/Multiprotocol cannot be\  
deleted as associated with S3 account
```

When you try to delete a share that doesn't exist, you also get an error:

```
CLUSTER_NAME> objectaccess share delete /vx/test1  
ACCESS ObjectAccess ERROR V-288-0 /vx/test1 does not exist
```

# Managing storage services

- [Chapter 26. Deduplicating data](#)
- [Chapter 27. Compressing files](#)
- [Chapter 28. Configuring Veritas Access SmartTier](#)
- [Chapter 29. Configuring cloud as a tier](#)
- [Chapter 30. Configuring SmartIO](#)
- [Chapter 31. Setting up Veritas Access Replication between two clusters](#)
- [Chapter 32. Using snapshots](#)
- [Chapter 33. Using instant rollbacks](#)
- [Chapter 34. Configuring NetBackup with Veritas Access](#)

# Deduplicating data

This chapter includes the following topics:

- [About data deduplication](#)
- [Best practices for using the Veritas Access deduplication feature](#)
- [Setting up deduplication](#)
- [Configuring deduplication](#)
- [Manually running deduplication](#)
- [Scheduling deduplication](#)
- [Setting deduplication parameters](#)
- [Removing deduplication](#)
- [Verifying deduplication](#)

## About data deduplication

Data deduplication is the process by which redundant data is eliminated to improve storage utilization. Using data deduplication, you can reduce the amount of storage required for storing user and application data. It is most effective in use-cases where many copies of very similar or even identical copies of data are stored. The deduplication feature in Veritas Access provides storage optimization for primary storage (storage of active data).

Each file in the configured file system is broken into user-configurable chunks for evaluating duplicates. The smaller the chunk size, the higher the percentage of sharing due to better chances of matches.

The first deduplication of a file system is always a full deduplication of the entire file system. This is an end-to-end deduplication process that identifies and eliminates

duplicate data. Any subsequent attempt to run deduplication on that file system results in incremental deduplication.

---

**Note:** Deduplication with a small chunk size increases the deduplication time and load on the system.

---

Veritas Access deduplication is periodic, that is, as per the user-configured frequency, redundant data in the file system is detected and eliminated.

## Use cases for deduplication

The following are potential use cases for Veritas Access file system deduplication:

- Microsoft Exchange mailboxes
- File systems hosting user home directories
- Virtual Machine Disk Format (VMDK) or virtual image stores.

## Relationship between physical and logical data on a file system

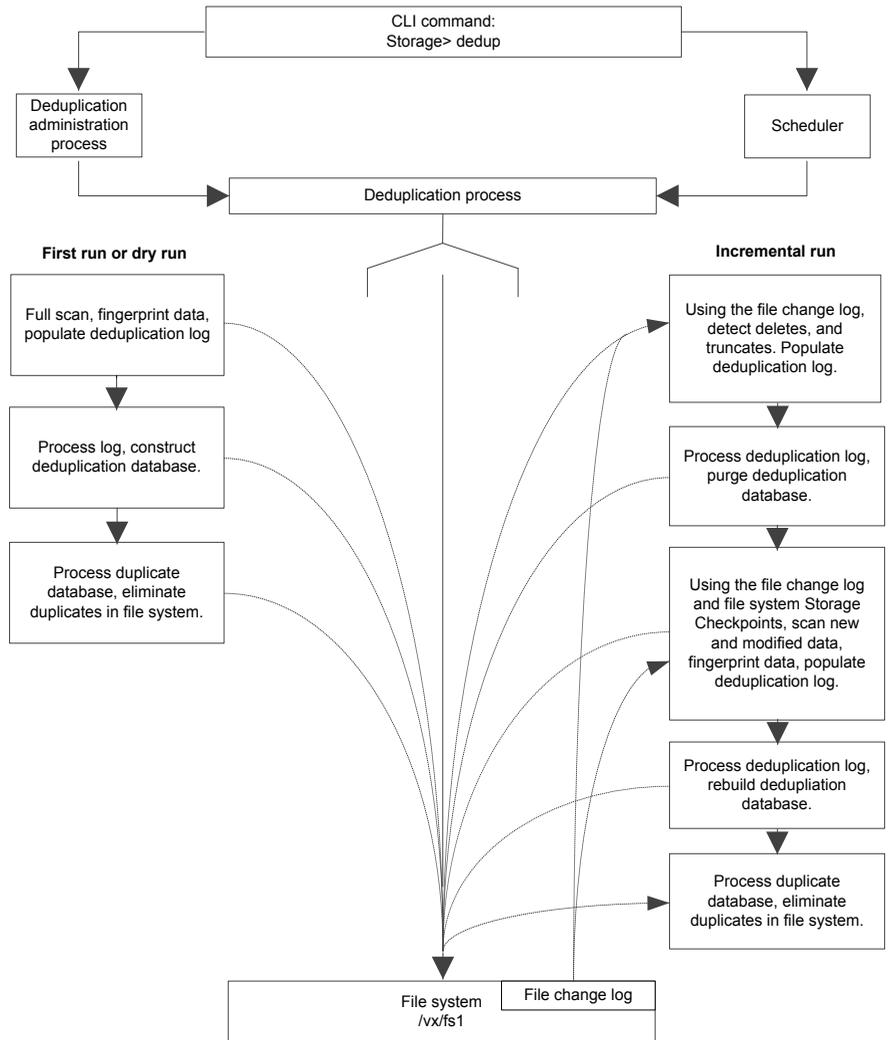
[Table 26-1](#) shows an estimated file system data size that can be supported for a Veritas Access deduplicated file system.

**Table 26-1** Relationship between physical and logical data on a file system for two billion unique fingerprints with various deduplication ratios

Fingerprint block size	Deduplication ratio	Unique signature per TB	Physical file system data size	Effective logical file system data size
4 K	50%	128 M	16 TB	32 TB
4 K	65%	90 M	23 TB	65 TB
4 K	80%	51 M	40 TB	200 TB
8 K	50%	64 M	32 TB	64 TB
8 K	65%	45 M	46 TB	132 TB
8 K	80%	25 M	80 TB	400 TB
16 K	50%	32 M	64 TB	128 TB
16 K	65%	22 M	93 TB	266 TB
16 K	80 %	13 M	158 TB	800 TB

## Overview of the deduplication workflow

**Figure 26-1** Overview of the deduplication workflow



The `Storage> dedup` commands perform administrative functions for the Veritas Access deduplication feature. The deduplication commands allow you to enable, disable, start, stop, and remove deduplication on a file system. You can also reset several deduplication configuration parameters and display the current deduplication status for your file system.

---

**Note:** Some configuration parameters can be set as local (specific to a file system) and or global (applicable to all deduplication-enabled file systems). Local parameters override the value of a global parameter.

---

## Best practices for using the Veritas Access deduplication feature

The following are best practices when using the Veritas Access deduplication feature:

- Deduplication is most effective when the file system block size and the deduplication block size are the same for file systems with block sizes of 4K and above. This also allows the deduplication process to estimate space savings more accurately.
- The smaller the file system block size and the deduplication block size, the higher is the time required for performing deduplication. Smaller block sizes such as 1 KB and 2 KB, increase the number of data fingerprints that the deduplication database has to store.  
Though the file system block size is data-dependent, the recommended block size for optimal deduplication is 4 KB for file systems less than 1 TB. For file systems 1 TB and above, it is 8 KB.
- For VMware NFS datastores that store Virtual Machine Disk Format (VMDK) images, a 4 KB block size is optimal.
- Compressed media files for images, music, and video, like JPEG, mp3, .MOV, and databases do not deduplicate or compress effectively.
- Home directory file systems are good candidates for deduplication.
- Deduplication is a CPU and I/O intensive process. It is a best practice to schedule deduplication when the load on your file systems is expected to be low.
- Evaluation of changes in the file system is done by the file system's File Change Log (FCL). Setting the frequency on a too infrequent basis may cause the FCL to rollover, thereby missing changes and deduplication opportunities to the file system.
- After enabling deduplication on file systems with existing data, the first deduplication run does a full deduplication. This can be time-consuming, and may take 12 to 15 hours per TB, so plan accordingly.
- The deduplication database takes up 1% to 7% of logical file system data. In addition, during deduplication processing, an additional but temporary storage space is required. Though 15% free space is enforced, it is recommended to

have 30% free space when the deduplication block size is less than 4096 (4 KB).

- If you plan to use the deduplication scheduler, you must have a Network Time Protocol (NTP) server enabled and configured.

## Setting up deduplication

This is an end-to-end sample scenario of deduplication.

### To deduplicate data

- 1 Ensure that the file system is deduplication-enabled. For example:

```
Storage> dedup list
```

See [“Configuring deduplication”](#) on page 446.

If the file system is not deduplication-enabled, you will need to enable it. For example:

```
Storage> dedup enable fs_name blksize
```

See [“Configuring deduplication”](#) on page 446.

- 2 (Optional) Once deduplication is enabled, you can set the CPU usage, the memory, and priority for the deduplication-enabled file system.

See [“Setting deduplication parameters”](#) on page 456.

- 3 Veritas recommends running a dryrun.

The dryrun provides you the space savings in percentage, if the threshold value is provided then the `fsdedup` command deduplicates data only if the expected savings cross the specified threshold.

```
Storage> dedup dryrun fs_name [threshold]
```

See [“Manually running deduplication”](#) on page 451.

---

**Note:** You cannot perform a dryrun on a file that has already been deduplicated.

---

- 4 You can either choose to start deduplication now or set up the deduplication schedule:

To start deduplication now

- Start deduplication now. For example:

```
Storage> dedup start fs_name [nodename]
```

See [“Manually running deduplication”](#) on page 451.

---

**Note:** If the system where you started deduplication crashes, the deduplication job fails over to one of the other nodes in the cluster. Run the `dedup status fs_name` command to find out the status. The `dedup status` command can temporarily show status as "FAILOVER" which means dedup job is currently being failed over and will resume shortly. dedup failover is applicable for deduplication jobs started with the `dedup start` command only. It is not applicable for scheduled dedup jobs.

---

To set up the deduplication schedule

- Set up the deduplication schedule. For example:

```
Storage> dedup schedule set fs_name hours day [freq]
```

See [“Scheduling deduplication”](#) on page 453.

- 5 You can check the status of the deduplication process. For example:

```
Storage> dedup status [fs_name]
```

See [“Verifying deduplication”](#) on page 459.

## Configuring deduplication

**To enable deduplication on a file system**

- ◆ To enable deduplication on a file system, enter the following:

```
Storage> dedup enable fs_name blksize
```

---

**Note:** Deduplication must be enabled for a file system before setting file system configuration parameters and schedules.

---

This command also re-enables a deduplication schedule for a file system.

Enabling deduplication does not automatically deduplicate a file system.

Deduplication has to be manually started by using the `Storage> dedup start` command or by setting up a schedule by using the `Storage> dedup set schedule` command.

*fs\_name* Specify the file system name for which you want to enable deduplication.

*blksize* Specify the deduplication block size of the file system in bytes, where possible values of bytes are the following:

- blksize=0 (Default)
- blksize=1024
- blksize=2048
- blksize=4096
- blksize=8192
- blksize=16384
- blksize=32768
- blksize=65536
- blksize=131072

Specify the deduplication block size in bytes, for example, 4096. The deduplication block size should be a power of 2. For example, 3 KB, is not a valid deduplication block size. The deduplication block size is a multiple of the file system's block size, and should be equal to or less than 128 KB.

0 is the default configuration for the deduplication block size.

If blksize=0 is specified while enabling deduplication, then if the file system block size is < 4096, then the deduplication block size is set to 4096. Otherwise, the deduplication block size is set to the same as the file system block size.

**Note:** Once the deduplication block size is set when enabling file system deduplication, the deduplication block size cannot be changed. The only way to change the deduplication block size is to remove deduplication on the file system and then re-enable deduplication on the file system.

For example, to enable deduplication on the file system fs1, enter:

```
Storage> dedup enable fs1 blksize=4096
```

```
ACCESS dedup SUCCESS V-288-0 Enabled dedup on file system fs1.  
Set memory, cpu, priority as required.
```

---

**Note:** For deduplication-enabled file systems, you are prompted to destroy the file system during `Storage> fs offline` and `Storage> fs destroy` operations.

---

For example:

```
Storage> dedup list
```

```
Default Priority CPU Memory
-----
                NORMAL      IDLE      2048M
```

```
Filesystem Priority CPU Granularity Enabled Schedule NodeList
-----
/vx/fs1     HIGH      YIELD      8192B YES      SET      node_01,node_02
/vx/fs2     LOW       IDLE       1024B YES      NONE     node_01,node_02
```

```
Storage> fs destroy fs1
```

```
ACCESS fs WARNING V-288-0 fs1 is deduplication configured.
```

```
Are you sure to destroy ? (yes/no) no
```

```
ACCESS fs ERROR V-288-0 Aborting fs destroy command
```

### To disable deduplication on a file system

- ◆ To disable deduplication on a file system, enter the following:

```
Storage> dedup disable fs_name
```

where *fs\_name* is the name of the deduplication-enabled file system that you want to disable.

Only the deduplication schedule is suspended for a deduplication-disabled file system. All other configuration parameters, for example, file system configuration, schedule, and the deduplication database remain intact.

---

**Note:** Keeping a file system deduplication-disabled for a significant period of time may reduce the effectiveness of deduplication when it is re-enabled.

---

### To list the deduplication-enabled file system or file systems

- ◆ To list the deduplication-enabled file system or file systems, enter the following:

```
Storage> dedup list fs_name
```

where *fs\_name* is the name of the deduplication-enabled file system that you want to list.

For example, to list the deduplication-enabled file systems, *fs1*, and then *fs2*, enter:

```
Storage> dedup list fs1
```

```
Priority          NORMAL
```

```
CPU                IDLE
Memory            2048M
Granularity       1024B
Enabled           YES
Schedule hours    Every hour
Schedule day interval Every day
Schedule frequency 1
NodeList          node_01,node_02
```

```
Storage> dedup list fs2
Priority          NORMAL
CPU              IDLE
Memory           2048M
Granularity      1024B
Enabled          YES
Schedule hours   00:00, 06:00, 12:00, 18:00, 23:00
Schedule day interval Every Monday
Schedule frequency 3
NodeList         node_01,node_02
```

Schedule hours are displayed as:

- \* - is displayed as "Every hour"
- \*/N - is displayed as "Every N hours"
- 0,6,12,18,23 are shown as "00:00, 06:00, 12:00, 18:00, 23:00"

---

**Note:** 0 is replaced by 00:00, 1 is replaced by 01:00, 23 is replaced by 23:00

---

Schedule day interval is displayed as:

- \* - is displayed as "Every day"
- \*/N - is displayed as "Every N days"
- 1 - is displayed as "Every Sunday"
- 2 - is displayed as "Every Monday"
- 3 - is displayed as "Every Tuesday"
- 4 - is displayed as "Every Wednesday"
- 5 - is displayed as "Every Thursday"
- 6 - is displayed as "Every Friday"
- 7 - is displayed as "Every Saturday"

If you issue the command without *fs\_name*, you get a list of all the deduplication-enabled file systems.

```
Storage> dedup list
```

```
Default Priority CPU Memory
-----
          NORMAL IDLE 2048M
```

```
Filesystem Priority CPU Granularity Enabled Schedule NodeList
-----
/vx/fs1     HIGH     YIELD    8192B YES     SET     node_01,node_02
/vx/fs2     LOW      IDLE     1024B YES     NONE    node_01,node_02
```

The `Default` column header indicates the global value (applicable to all deduplication-enabled file systems). For example, if you have not set `Priority`, `CPU`, and `Memory` for file system `fs1`, the deduplication process uses the global value. Veritas Access deduplication uses the default values for global settings options. Local parameters override the value of global parameters.

# Manually running deduplication

## To create a deduplication dryrun

- ◆ To create a deduplication dryrun, enter the following command:

```
Storage> dedup dryrun fs_name [threshold]
```

The `Storage> dedup dryrun` command is useful for determining the statistics/potential savings on the file system data if actual deduplication is performed. Most accurate statistics are obtained when the file system block size and the deduplication block size are the same.

---

**Note:** You cannot perform a dryrun on a file system that has already been deduplicated.

---

*fs\_name* Specify the file system name for which you want to create a dryrun.

*threshold* Specify the threshold percentage in the range of [0-100].

A dryrun is automatically converted to the actual deduplication if the dryrun meets the threshold value. For example, if you specified a threshold value of 40%, and if deduplication results in a space savings of  $\geq 40\%$ , then the dryrun is automatically converted to the actual deduplication

To check whether the deduplication dryrun reaches to a threshold value of 60%, enter the following:

```
Storage> dedup dryrun fs1 60
```

### To start the deduplication process

- ◆ To manually start the deduplication process, enter the following:

```
Storage> dedup start fs_name [nodename]
```

where *fs\_name* is the name of the file system where you want to start the deduplication process and *nodename* is the node in the cluster where you want to start deduplication. You can run deduplication on any node in the cluster.

---

**Note:** If the system where you started deduplication crashes, the deduplication job fails over to one of the other nodes in the cluster. Run the `dedup status fs_name` command to find out the status. The `dedup status` command can temporarily show status as "FAILOVER" which means dedup job is currently being failed over and will resume shortly. dedup failover is applicable for deduplication jobs started with the `dedup start` command only. It is not applicable for scheduled dedup jobs.

---

When the deduplication process is started for the first time, a full scan of the file system is performed. Any subsequent attempt to run deduplication requires an incremental scan only.

For example:

```
Storage> dedup start fs1 node_01
```

---

**Note:** When deduplication is running on a file system, you run the `Storage> fs offline` or `Storage> fs destroy` commands, these operations can proceed only after deduplication is stopped by using the `Storage> dedup stop` command.

---

### To stop the deduplication process

- ◆ To stop the deduplication process running on a file system, enter the following command:

```
Storage> dedup stop fs_name
```

where *fs\_name* is the name of the file system where you want to stop the deduplication process.

---

**Note:** The deduplication process may not stop immediately as a consistent state is ensured while stopping. Use the `Storage> dedup status` command to verify if the deduplication process has stopped.

---

# Scheduling deduplication

## To set the deduplication schedule

- 1 To set the deduplication schedule, enter the following:

```
Storage> dedup schedule set fs_name
      hours
      day [freq]
```

The `Storage> dedup schedule set` command can only be set as a local parameter.

Two categories of schedules are allowed: run periodicity and type periodicity. The granularity of the schedule is limited to the time of day and the day of the month.

***fs\_name*** Specify the file system where you want to set the deduplication schedule.

***hours*** Specify the `hours` value for setting the duplication schedule.

There are three types of values for the `hours` field:

- \* - indicates every hour.
- \*/N - indicates every Nth hour, where N is in the range [1-12].
- You can also specify 5 comma-separated hours in the range of [0-23].

For example:

```
Storage> dedup schedule modify fs1 0,6,12,18,23 2 3
ACCESS dedup SUCCESS V-288-0 Schedule modify on
file system fs1.
```

*day* Specify the interval in days for setting the deduplication schedule.

There are three types of values for the `day` field:

- \* - indicates every day.
- \*/N - indicates every Nth day, where N is in the range of [1-15].
- Any number in the range of [1-7] where:
  - 1 - Sunday
  - 2 - Monday
  - 3 - Tuesday
  - 4 - Wednesday
  - 5 - Thursday
  - 6 - Friday
  - 7 - Saturday

The deduplication scheduler will only pick up the schedule if the schedule is enabled for deduplication.

*freq* Specify the frequency to run the deduplication schedule in the range of [1-5]. The default frequency is [1].

This value controls deduplication load on the file system by distributing phases of deduplication across various runs, and potentially across systems in the cluster. A value of 4 means, every 4th run deduplicates the file system, whereas the other runs consolidate the changes.

## 2 When you set a deduplication schedule, keep in mind the following:

- If the hour value for a schedule is set as \*/N, then the deduplication scheduler picks up the schedule every Nth hour starting from 00:00 and ending at 23:00. The hour schedule resets at end of day.  
For example, if the hour value is \*/5, then the schedule time will be 00:00, 05:00, 10:00, 15:00, and 20:00 hours. On the next day, the schedule repeats at the same times.
- If day value for a schedule is set as \*/N, then the deduplication scheduler picks up the schedule every Nth day starting from the 1st day of the month and ending with the last day of the month. The day schedule resets at end of each month.  
For example, if the day value is \*/5, then the schedule day is on the 1st, 6th, 11th, 16th, 21st, 26th, and 31st days for a 31-day month. For the next month, the schedule repeats on the same days.
- For both the hour and day schedule, the \* and \*/1 values are interchangeable. They indicate every hour and every day.

## To modify the deduplication schedule

- ◆ To modify the deduplication schedule, enter the following:

```
Storage> dedup schedule modify fs_name
      hours
      day
      freq
```

*fs\_name* Specify the file system where you want to modify the deduplication schedule.

*hours* Specify the `hours` value for modifying the deduplication schedule.

There are three types of values for the `hours` field:

- \* - indicates every hour.
- \*/N - indicates every Nth hour, where N is in the range [1-12].
- You can also specify 5 comma-separated hours in the range of [0-23].

For example:

```
Storage> dedup schedule modify fs1 0,6,12,18,23 2 3
ACCESS dedup SUCCESS V-288-0 Schedule modify on
file system fs1.
```

*day* Specify the interval in days for modifying the deduplication schedule.

There are three types of values for the `day` field:

- \* - indicates every day.
- \*/N - indicates every Nth hour, where N is in the range [1-15].
- Any number in the range of [1-7] where:
  - 1 - Sunday
  - 2 - Monday
  - 3 - Tuesday
  - 4 - Wednesday
  - 5 - Thursday
  - 6 - Friday
  - 7 - Saturday

**Note:** The deduplication scheduler will only pick up the schedule if the schedule is enabled for deduplication.

*freq* Specify the frequency to run the deduplication schedule in the range of [1-5].

**To delete the deduplication schedule**

- ◆ To delete the deduplication schedule, enter the following:

```
Storage> dedup schedule delete fs_name
```

where *fs\_name* is the name of the file system that you want to delete.

## Setting deduplication parameters

**To set the CPU usage for the deduplication-enabled file system**

- ◆ To set the CPU usage for the file system, enter the following:

```
Storage> dedup set cpu cpuvalue fs_name
```

*cpuvalue*

Specify the CPU usage behavior for the deduplication-enabled file system.

The following are the available values:

- IDLE - indicates that the deduplication process consumes as much CPU processing as is available. For example, if the CPUs are IDLE, then the deduplication process takes all of the idle CPUs, and performs the deduplication job faster. CPU usage may reach 100% on each available CPU.
- YIELD (default) - indicates that the deduplication process yields the CPU periodically; that is, even if the CPUs are not busy, the deduplication process relinquishes the CPU. More time may be taken for the same job in some scenarios. However, the yield value ensures that the deduplication process does not hang onto the CPU, or cause CPU usage spikes.

*fs\_name*

Specify the deduplication-enabled file system for which you want to set the CPU usage.

**Note:** If a file system name is specified, the `Storage> dedup set cpu` command sets the CPU value for that file system. Otherwise, the CPU value is applicable to all file systems, which have not overridden the CPU value.

**To set the deduplication memory allocation limit for the deduplication-enabled file system**

- ◆ To set the deduplication memory limit in MB for the deduplication-enabled file system, enter the following:

```
Storage> dedup set memory memvalue
```

where *memvalue* is the memory value in MB, for example, 1024.

The *memvalue* controls the maximum memory per deduplication process.

---

**Note:** Care must be taken to increase *memvalue* if large file systems are present. Otherwise, deduplication efficiency may be affected. Since this is a limit value, only the required memory is consumed for smaller file system deduplication jobs. Note that scheduled deduplication jobs start deduplication based on the available memory; therefore, if available RAM in the system falls below the configured memory allocation limit for deduplication, the deduplication scheduler on that system postpones the scheduled deduplication. At this point, other systems with available memory starts deduplication. If the job remains postponed for 1 hour, the job will be abandoned.

---

**To set the deduplication priority for the deduplication-enabled file system**

- ◆ To set the deduplication priority (importance) for the deduplication-enabled file system, enter the following:

```
Storage> dedup set priority priorityvalue [fs_name]
```

*priorityvalue*

Specify the importance of deduplication for the file system. The setting of this parameter is local (specific to a file system). The *priorityvalue* parameter is used by the deduplication scheduler to evaluate if starting deduplication at the scheduled time is appropriate or not based on the state of the file system at that time.

*priorityvalue* is also a load-balancing mechanism whereby a less-loaded system in the cluster may pick up a scheduled deduplication job.

Available values are the following:

- LOW (default) - indicates that if the system has sustained CPU usage of 50% or more in the last one hour, the file systems marked as LOW have their deduplication schedules skipped with a message in the syslog
- NORMAL - indicates that if the system has sustained CPU usage of 80% or more in the last one hour, the file systems marked as NORMAL have their deduplication schedules skipped with a message in the syslog
- HIGH - indicates that starting deduplication is a must for this file system, and without evaluating any system state, deduplication is started at the scheduled time.

*fs\_name*

Specify the file system where you want to set the deduplication priority.

## Removing deduplication

### To remove deduplication configuration-related information from the specified file system

- ◆ Enter the following:

```
Storage> dedup remove fs_name
```

where *fs\_name* is the name of the file system for which you want to remove deduplication.

This command removes all configurations and the deduplication database for the specified file system.

---

**Note:** This operation cannot be undone, and re-running deduplication on your file system may take a significant amount of time.

---

# Verifying deduplication

To obtain status information for a specified deduplicated-enabled file system or all deduplicated-enabled file systems

- ◆ Enter the following command:

```
Storage> dedup status [fs_name]
```

where *fs\_name* is the specified deduplicated-enabled file system for which you want to obtain current status information.

If you issue the command without *fs\_name*, you get status information for all deduplicated-enabled file systems. For example:

```
Storage> dedup status
Filesystem Saving Status      Node      Type      Details
-----
/vx/fs1      00%      COMPLETED node_01  MANUAL  2011/05/17 16:57:16 End full scan with error
/vx/fs2      00%      COMPLETED node_01  MANUAL  2011/05/17 16:57:32 End detecting duplicates
                                                and filesystem changes 0
```

If you issue the command with *fs\_name*, you get the detailed status information for the specified file system, along with any error messages or warnings.

```
Storage> dedup status fs2
Filesystem Saving Status      Node      Type      Details
-----
/vx/fs2      00%      COMPLETED node_01  MANUAL  2011/05/17 16:57:32 End detecting
                                                duplicates and filesystem changes 0
                                                2011/05/17 16:57:17 DEDUP_INFO Using
                                                FP block size = 4096 Mode = 0
```

The following describes the output from the `Storage> dedup status` command:

Filesystem            Displays the directory where the file system is mounted.

Savings	<p>Displays the savings as a percentage. The value can mean different things during the course of deduplication.</p> <p>When the deduplication is in a COMPLETED state, or when the deduplication process is computing the expected deduplication, the value in this column shows the actual sharing in the file system. However, when the expected deduplication calculation is complete, this column value shows the expected deduplication. The expected deduplication calculation is based on user data only; therefore, at the end of deduplication, the saving percentage may vary from the expected deduplication percentage. This is because the actual file system deduplication percentage not only takes into consideration the user data, but also file system and deduplication metadata. This difference may be pronounced if the user data is very small. For a failed deduplication, the value is undefined.</p>
Status	<p>Displays one of the following status values:</p> <ul style="list-style-type: none"><li>■ RUNNING</li><li>■ COMPLETED</li><li>■ STOPPED</li><li>■ FAILED</li><li>■ FAILOVER</li><li>■ NONE - indicates that deduplication has not been previously run on this file system.</li></ul>
Node	<p>Indicates the node name where the deduplication job is either running or has completed for a file system.</p>
Type	<p>The following are the types of deduplication jobs:</p> <ul style="list-style-type: none"><li>■ MANUAL - the deduplication job is started by using either the <code>Storage&gt; dedup start</code> command or the <code>Storage&gt; dedup dryrun</code> command.</li><li>■ SCHEDULED - the deduplication job is started by the deduplication scheduler.</li></ul>

**Details**

Displays the status of the file system deduplication activity.

The deduplication process writes its status in the status log. The relevant status log is displayed in this column. For a long-running deduplication process, the status log may also show the actual file system sharing as a progress indicator. This actual file system sharing percentage along with the expected saving percentage in the `Saving` column gives a good estimate of the progress. When displaying deduplication status for a specific file system, any errors, or warnings for the deduplication run are also shown. The `Details` column gives a detailed idea of what to look for in case of any issues.

# Compressing files

This chapter includes the following topics:

- [About compressing files](#)
- [Use cases for compressing files](#)
- [Best practices for using compression](#)
- [Compression tasks](#)

## About compressing files

Compressing files reduces the space used, while retaining the accessibility of the files and being transparent to applications. Compressed files look and behave almost exactly like uncompressed files: the compressed files have the same name, and can be read and written as with uncompressed files. Reads cause data to be uncompressed in memory, only; the on-disk copy of the file remains compressed. In contrast, after a write, the new data is uncompressed on disk.

Only user data is compressible. You cannot compress Veritas File System (VxFS) metadata.

After you compress a file, the inode number does not change, and file descriptors opened before the compressions are still valid after the compression.

Compression is a property of a file. Thus, if you compress all files in a directory, for example, any files that you later copy into that directory do not automatically get compressed. You can compress the new files at any time by compressing the files in the directory again.

You compress files with the `storage> compress` command.

See [“Compression tasks”](#) on page 464.

See the `storage_compress(1)` manual page.

To compress files, you must have VxFS file systems with disk layout Version 8 or later.

See [“Upgrading disk layout versions”](#) on page 394.

---

**Note:** When you back up compressed files to tape, the backup program stores the data in an uncompressed format. The files are uncompressed in memory and subsequently written to the tape. This results in increased CPU and memory usage when you back up compressed files.

---

## About the compressed file format

A compressed file is a file with compressed extents. A `compress` call compresses all extents of a file. However, writes to the file cause the affected extents to get uncompressed; the result can be files with both compressed and uncompressed extents.

## About the file compression attributes

When you compress a file with the `Storage> compress` command, `compress` attaches the following information to the inode:

- Compression algorithm
- Compression strength, which is a number from 1 to 9
- Compression block size

This information is referred to as the file compression attributes. The purpose of the attributes are to collect the parameters used to create the compressed file. The information can then be read by a backup program.

The file compression attributes guarantee that a particular compressed file can only use one type and strength of compression. Recompressing a file using different attributes fails. To change the file compression attributes, you must explicitly uncompress first, and then recompress with the new options, even in the case where all extents are already uncompressed.

The file compression attributes do not indicate if all extents are compressed. Some extents might be incompressible, and other extents or even all extents might be uncompressed due to writes, but the file compression attributes remain. Only an explicit file uncompression can remove the attributes.

## About the file compression block size

The file compression algorithm compresses data in the specified block size, which defaults to 1MB. Each compression block has its own extent descriptor in the inode. If the file or the last extent is smaller than the compression block size, then that smaller size gets compressed. The maximum block size is 1MB.

Extents with data that cannot be compressed are still marked as compressed extents. Even though such extents cannot be compressed, marking these extents as compressed allows successive compression runs to skip these extents to save time. Shared extents cannot be compressed and do not get marked as compressed. Since the file compression algorithm looks at fixed-size blocks, the algorithm finds these incompressible extents in units of the file compression block size.

## Use cases for compressing files

The following list contains common use case categories:

- If files are old and not accessed frequently. For example:
  - Compress database archive logs which are older than 8 days.
  - Compress jpeg files which are not accessed in 30 days.

## Best practices for using compression

Best practices for using compression:

- Schedule compression during non-peak hours.

## Compression tasks

**Table 27-1** Compression tasks

How to	Task
How to compress a file or all files in a directory	See <a href="#">“Compressing files”</a> on page 465.
How to scheduled compression jobs	See <a href="#">“Scheduling compression jobs”</a> on page 466.
How to list compressed files	See <a href="#">“Listing compressed files”</a> on page 469.
How to show the scheduled compression job	See <a href="#">“Scheduling compression jobs”</a> on page 466.

**Table 27-1** Compression tasks (*continued*)

How to	Task
How to uncompress a file or all files in a directory	See <a href="#">“Uncompressing files”</a> on page 470.
How to modify the scheduled compression	See <a href="#">“Modifying the scheduled compression”</a> on page 471.
How to remove the specified schedule.	See <a href="#">“Removing the specified schedule”</a> on page 473.
How to stop the schedule for a file system.	See <a href="#">“Stopping the schedule for a file system”</a> on page 473.
How to remove the pattern-related rule for a file system	See <a href="#">“Removing the pattern-related rule for a file system”</a> on page 473.
How to remove the modification age (age-based) related rule for a file system	See <a href="#">“Removing the modified age related rule for a file system”</a> on page 474.

## Compressing files

You can compress a file or compress all files in a directory.

### To compress a file

- ◆ Compress a file:

```
Storage> compress file fs_name file_or_dir resource_level algorithm
```

where *fs\_name* is the name of the file system.

where *file\_or\_dir* is the name of the file or directory.

where *resource\_level* is either `low`, `medium`, or `high`.

where *algorithm* is the file compression algorithm strength [1–9]. For example, you specify strength gzip-3 compression as "3".

See [“About the file compression attributes”](#) on page 463.

For example:

```
Storage> compress file tpcc_data1 system.dbf medium 3
ACCESS compression Success V-288-999 Compression Completed
```

### To compress all files in a directory

- ◆ Compress all files in a directory:

```
Storage> compress file fs_name file_or_dir resource_level algorithm
```

For example:

```
Storage> compress file tpcc_data1 data_dir high 8 *.dbf  
ACCESS compression Success V-288-999 Compression Completed
```

## Scheduling compression jobs

Schedule compression jobs lets you compress pattern-based and age-based compression.

## To schedule compression

### 1 Create a scheduled compression:

```
Storage> compress schedule create new_schedule duration min \  
[hour] [day_of_month] [month] [day_of_week] [node]
```

where *new\_schedule* is the name of the schedule.

where *duration* is the duration specified in hours (1 or more).

where *min* is the minutes.

where *hour* is the hours.

where *day* is the day of the month.

where *month* is the month.

where *day\_of\_week* is the day of the week.

where *node* is the name of the node or you can use "any".

For example:

```
Storage> compress schedule create schedule1 3 0 1 * * 6
```

This creates a schedule called "schedule1" that starts compression at 1:00 am every Friday and runs for only 3 hours.

### 2 Start the schedule for a given file system:

```
Storage> compress schedule start fs_name schedule_name \  
resource_level algorithm
```

where *fs\_name* is the name of the file system.

where *schedule\_name* is the name of the schedule.

where *resource\_level* is either low, medium, or high.

where *algorithm* is the file compression algorithm strength [1-9]. For example, you specify strength gzip-3 compression as "3".

For example:

```
Storage> compress schedule start fs1 schedule1 medium 3
```

### 3 Show the scheduled compression:

```
Storage> compress schedule show new_schedule
```

For example:

```
Storage> compress schedule show schedule1
Name           Node Duration Minute Hour Day Month WeekDay
====          =====
schedule1     any  3hours    0     1  *   *     6
```

### 4 (Optional) Create a pattern for the file system.

```
Storage> compress pattern create fs_name pattern
```

where *pattern* is the extensions of the file names separated by ",", For example, \*.arc, \*.dbf, \*.tmp.

For example:

```
Storage> compress pattern create tpcc_data1 *.arc, *.tmp
ACCESS compression Success V-288-999 Pattern created
```

**5** (Optional) Create a modification age rule for the file system.

```
Storage> compress modage create fs_name mod_age
```

where *mod\_age* is the modification age (age-based) specified units are in days.

For example:

```
Storage> compress modage create tpcc_data1 7
ACCESS compression Success V-288-999 Modage created
```

**6** If you performed step 4 or 5, you can list the schedule details for the file system:

```
Storage> compress schedule list fs_name
```

For example:

```
Storage> compress schedule list tpcc_data1

Schedule Information for tpcc_data1
=====
Name           Node Duration Minute Hour Day Month WeekDay
=====
schedule1     any 3hour(s) 0      1   *   *       6
Mod Age Algorithm Resource pattern
=====
7             3      medium  *.arch,*.tmp
```

## Listing compressed files

### To list compressed files

- ◆ List compressed files:

```
Storage> compress list fs_name file_or_dir
```

where *fs\_name* is the name of the file system.

where *file\_or\_dir* is the name of the file or directory.

For example:

```
Storage> compress list tpcc_data1 system.dbf
%Comp  Physical    Logical    %Exts    Alg-Str  BSize  Filename
81%    38.2 MB      198.0 MB  100%     gzip-3   1024k  system.dbf
```

## Showing the scheduled compression job

### To show the scheduled compression job

- ◆ Show the scheduled compression job

```
Storage> compress schedule show new_schedule
```

where *new\_schedule* is the name of the schedule.

For example:

```
Storage> compress schedule show schedule1
```

Name	Node	Duration	Minute	Hour	Day	Month	WeekDay
====	====	=====	=====	====	==	=====	=====
schedule1	any	3hours	0	1	*	*	6

## Uncompressing files

### To uncompress a file

- ◆ Uncompress a file:

```
Storage> uncompress file fs_name file_or_dir resource_level
```

where *fs\_name* is the name of the file system.

where *file\_or\_dir* is the name of the file or directory.

where *resource\_level* is either low, medium, or high.

For example:

```
Storage> uncompress file tpcc_data1 system.dbf high
```

```
ACCESS compression Success V-288-999 Uncompression completed
```

### To uncompress all files in a directory

- ◆ Uncompress all files in a directory:

```
Storage> uncompress file fs_name file_or_dir resource_level
```

For example:

```
Storage> uncompress file tpcc_data1 data_dir high
```

```
ACCESS compression Success V-288-999 Uncompression completed
```

## Modifying the scheduled compression

### To change the scheduled compression

- 1 Stops the schedule for the file system:

```
Storage> compress schedule stop fs_name
```

where *fs\_name* is the name of the file system.

For example:

```
Storage> compress schedule stop tpcc_data1
```

- 2 Remove specified schedule:

```
Storage> compress schedule remove new_schedule
```

For example:

```
Storage> compress schedule remove schedule1
```

### 3 Create a scheduled compression:

```
Storage> compress schedule create new_schedule duration min \  
[hour] [day_of_month] [month] [day_of_week] [node]
```

where *new\_schedule* is the name of the schedule.

where *duration* is the duration specified in hours (1 or more).

where *min* is the minutes.

where *hour* is the hours.

where *day* is the day of the month.

where *month* is the month.

where *day\_of\_week* is the day of the week.

where *node* is the name of the node or you can use "any".

For example:

```
Storage> compress schedule create schedule2 3 0 2 * * 6
```

This creates a schedule called "schedule2" that starts compression at 2:00 am every Friday and runs for only 3 hours.

### 4 Start the schedule for a given file system:

```
Storage> compress schedule start fs_name schedule_name \  
resource_level algorithm
```

where *fs\_name* is the name of the file system.

where *schedule\_name* is the name of the schedule.

where *resource\_level* is either low, medium, or high.

where *algorithm* is the file compression algorithm strength [1-9]. For example, you specify strength gzip-3 compression as "3".

For example:

```
Storage> compress schedule start fs1 schedule2 medium 3
```

## Removing the specified schedule

### To remove the specified schedule

- ◆ Enter the following:

```
Storage> compress schedule remove new_schedule
```

where *new\_schedule* is the name of the schedule.

For example:

```
Storage> compress schedule remove schedule1
```

## Stopping the schedule for a file system

### To stop the schedule for a file system

- ◆ Enter the following:

```
Storage> compress schedule stop fs_name
```

where *fs\_name* is the name of the file system.

For example:

```
Storage> compress schedule stop tpcc_data1
```

## Removing the pattern-related rule for a file system

### To remove the pattern-related rule a named file system

- ◆ Enter the following:

```
Storage> compress pattern remove fs_name
```

where *fs\_name* is the name of the file system.

For example:

```
Storage> compress pattern remove tpcc_data1
```

## Removing the modified age related rule for a file system

### To remove the modified age related rule for a file system

- ◆ Enter the following:

```
Storage> compress modage remove fs_name
```

where *fs\_name* is the name of the file system.

For example:

```
Storage> compress modage remove tpcc_data1
```

# Configuring Veritas Access SmartTier

This chapter includes the following topics:

- [About Veritas Access SmartTier](#)
- [How Veritas Access uses SmartTier](#)
- [Adding tiers to a file system](#)
- [Adding or removing a column from a secondary tier of a file system](#)
- [Configuring a mirror to a tier of a file system](#)
- [Listing all of the files on the specified tier](#)
- [Displaying a list of SmartTier file systems](#)
- [Displaying the tier location of a specified file](#)
- [About tiering policies](#)
- [About configuring the policy of each tiered file system](#)
- [Configuring the policy of each tiered file system](#)
- [Best practices for setting relocation policies](#)
- [Relocating a file or directory of a tiered file system](#)
- [About configuring schedules for all tiered file systems](#)
- [Configuring schedules for tiered file systems](#)
- [Displaying the files that may be moved or pruned by running a policy](#)

- [Allowing metadata information on the file system to be written on the secondary tier](#)
- [Restricting metadata information to the primary tier only](#)
- [Removing a tier from a file system](#)

## About Veritas Access SmartTier

The Veritas Access SmartTier feature makes it possible to allocate two tiers of storage to a file system.

The following features are part of the Veritas Access SmartTier solution:

- Relocate files between primary and secondary tiers automatically as files age and become less business critical.
- Prune files on secondary tiers automatically as files age and are no longer needed.
- Promote files from a secondary storage tier to a primary storage tier based on I/O temperature.
- Retain original file access paths to eliminate operational disruption, for applications, backup procedures, and other custom scripts.
- Let you manually move folders, files and other data between storage tiers.
- Enforce the policies that automatically scan the file system and relocate files that match the appropriate tiering policy.

In Veritas Access, there are two predefined tiers for storage:

- Current active tier 1 (primary) storage.
- Tier 2 (secondary) storage for aged or older data.

To configure Veritas Access SmartTier, add tier 2 (secondary) storage to the configuration. Specify where the archival storage resides (storage pool) and the total size.

Files can be moved from the active storage after they have aged for a specified number of days, depending on the policy selected. The number of days for files to age (not accessed) before relocation can be changed at any time.

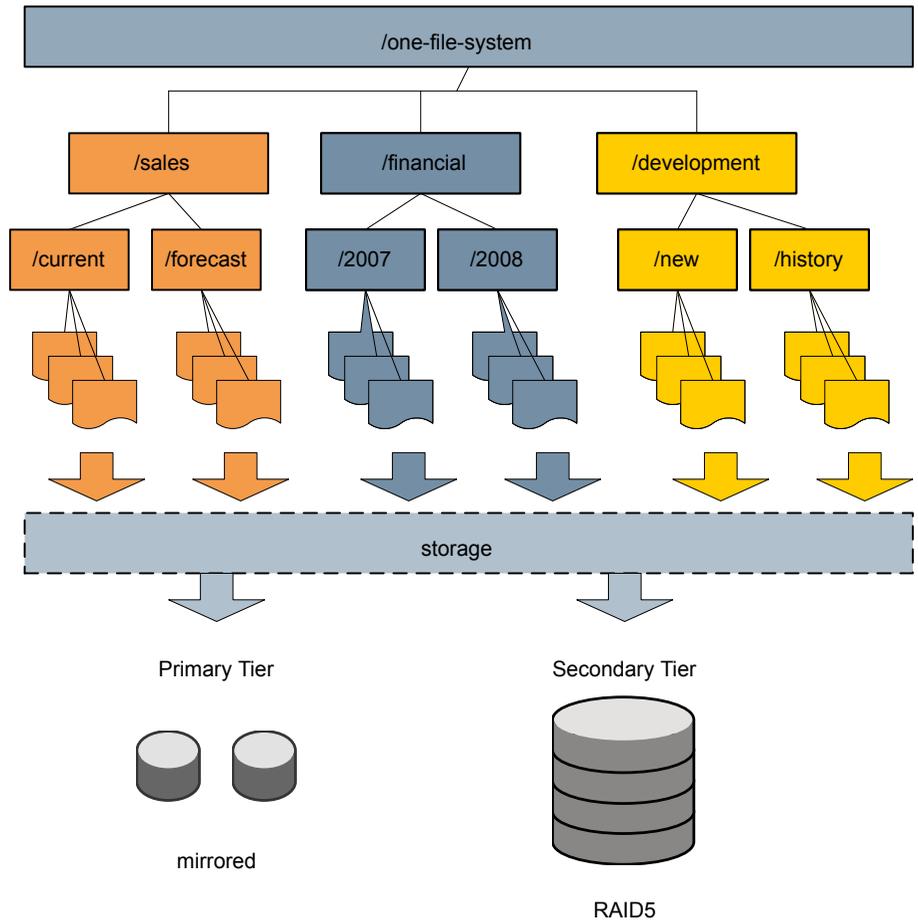
---

**Note:** An aged file is a file that exists without being accessed.

---

[Figure 28-1](#) depicts the features of Veritas Access and how it maintains application transparency.

**Figure 28-1** SmartTier features



If you are familiar with Veritas Volume Manager (VxVM), every Veritas Access file system is a multi-volume file system (one file system resides on two volumes). The SmartTier tiers are predefined to simplify the interface. When an administrator wants to add storage tiering, a second volume is added to the volume set, and the existing file system is encapsulated around all of the volumes in the file system.

## How Veritas Access uses SmartTier

Veritas Access provides two types of tiers:

- Primary tier

- Secondary tier

Each newly created file system has only one primary tier initially. This tier cannot be removed.

For example, the following operations are applied to the primary tier:

```
Storage> fs addmirror
```

```
Storage> fs growto
```

```
Storage> fs shrinkto
```

The `Storage> tier` commands manage file system tiers.

All `Storage> tier` commands take a file system name as an argument and perform operations on the combined construct of that file system.

The Veritas Access file system default is to have a single storage tier. An additional storage tier can be added to enable storage tiering. A file system can only support a maximum of two storage tiers.

`Storage> tier` commands can be used to perform the following:

- Adding/removing/modifying the secondary tier
- Setting policies
- Scheduling policies
- Locating tier locations of files
- Listing the files that are located on the primary or the secondary tier
- Moving files from the secondary tier to the primary tier
- Allowing metadata information on the file system to be written on the secondary tier
- Restricting metadata information to the primary tier only

## Adding tiers to a file system

You can add the following types of tiers to file systems:

- simple
- mirrored
- striped
- mirrored-stripe
- striped-mirror

---

**Note:** If a rollback exists for the file system, adding a tier can cause inconsistencies in the rollback hierarchy. The recommended method is to create the tier first and then create the rollback.

---

### To add a second tier to a file system

- ◆ To add a tier to a file system where the layout is "simple" (concatenated), enter the following:

```
Storage> tier add simple fs_name size pool1[,disk1,...]
```

### To add a mirrored tier to a file system

- ◆ To add a mirrored tier to a file system, enter the following:

```
Storage> tier add mirrored fs_name size nmirrors  
pool1[,disk1,...] [protection=disk|pool]
```

For example:

```
Storage> tier add mirrored fs1 100M 2 pool3,pool4  
100% [#] Creating mirrored secondary tier of filesystem
```

### To add a striped tier to a file system

- ◆ To add a striped tier to a file system, enter the following:

```
Storage> tier add striped fs_name size ncolumns  
pool1[,disk1,...] [stripeunit=kilobytes]
```

### To add a mirrored-striped tier to a file system

- ◆ To add a mirrored-striped tier to a file system, enter the following:

```
Storage> tier add mirrored-stripe fs_name size nmirrors ncolumns  
pool1[,disk1,...] [protection=disk|pool] [stripeunit=kilobytes]
```

### To add a striped-mirror tier to a file system

- ◆ To add a striped-mirror tier to a file system, enter the following:

```
Storage> tier add striped-mirror fs_name size nmirrors ncolumns  
pool1[,disk1,...] [protection=disk|pool] [stripeunit=kilobytes]
```

<code>fs_name</code>	Specifies the name of the file system to which the mirrored tier is added. If the specified file system does not exist, an error message is displayed.
----------------------	--

**Adding or removing a column from a secondary tier of a file system**

size	Specifies the size of the tier to be added to the file system (for example, 10m, 10M, 25g, 100G).
ncolumns	Specifies the numbers of columns to add to the striped tiered file system.
nmirrors	Specifies the number of mirrors to be added to the tier for the specified file system.
pool1[,disk1,...]	<p>Specifies the pool(s) or disk(s) that is used for the specified tiered file system. If the specified pool or disk does not exist, an error message is displayed. You can specify more than one pool or disk by separating the pool or the disk name with a comma, but do not include a space between the comma and the name.</p> <p>The disk needs to be part of the pool or an error message is displayed.</p>
protection	<p>If no protection level is specified, <code>disk</code> is the default protection level.</p> <p>The protection level of the second tier is independent of the protection level of the first tier.</p> <p>Available options are:</p> <ul style="list-style-type: none"> <li>■ <code>disk</code> - If <code>disk</code> is entered for the protection field, then mirrors are created on separate disks. The disks may or may not be in the same pool.</li> <li>■ <code>pool</code> - If <code>pool</code> is entered for the protection field, then mirrors are created in separate pools. If not enough space is available, then the file system is not created.</li> </ul>
stripeunit=kilobytes	Specifies a stripe width of either 128K, 256k, 512K, 1M, or 2M. The default stripe width is 512K.

## Adding or removing a column from a secondary tier of a file system

You can add a column to a secondary tier of a file system.

### To add a column to a secondary tier of a file system

- ◆ To add a column to a secondary tier of a file system, enter the following:

```
Storage> tier addcolumn fs_name ncolumns pool_or_disk_name
```

*fs\_name* Specifies the file system for which you want to add a column to a secondary tier of the file system.

*ncolumn* Specifies the number of columns that you want to add to the secondary tier of the file system.

**Note:** In the case of striped file systems, the number of disks that are specified should be equal to the number of columns (*ncolumns*).

**Note:** In the case of mirrored-striped and striped-mirrored file systems, the disks that are specified should be equal to (*ncolumns \* number\_of\_mirrors\_in\_fs*).

*pool\_or\_disk\_name* Specifies the pool or the disk name for the tiered file system.

For example, to add two columns to the secondary tier of file system *fs1*, enter the following:

```
Storage> tier addcolumn fs1 2 pool3
```

### To remove a column from a secondary tier of a file system

- ◆ To remove a column from a secondary tier of a file system, enter the following:

```
Storage> tier rmcolumn fs_name
```

where *fs\_name* is the name of the tiered file system, the secondary tier of which you want to remove the column from.

For example:

```
Storage> tier rmcolumn fs1
```

## Configuring a mirror to a tier of a file system

### To add a mirror to a tier of a file system

- ◆ To add a mirror to a tier of a file system, enter the following:

```
Storage> tier addmirror fs_name pool1[,disk1,...]  
[protection=disk|pool]
```

<code>fs_name</code>	Specifies the file system to which a mirror is added. If the specified file system does not exist, an error message is displayed.
<code>pool1[,disk1,...]</code>	<p>Specifies the pool(s) or disk(s) that are used as a mirror for the specified tiered file system. You can specify more than one pool or disk by separating the name with a comma. But do not include a space between the comma and the name.</p> <p>The disk needs to be part of the pool or an error message is displayed.</p>
<code>protection</code>	<p>If no protection level is specified, <code>disk</code> is the default protection level.</p> <p>Available options are:</p> <ul style="list-style-type: none"> <li>■ <code>disk</code> - If <code>disk</code> is entered for the protection field, then mirrors are created on separate disks. The disks may or may not be in the same pool.</li> <li>■ <code>pool</code> - If <code>pool</code> is entered for the protection field, then mirrors are created in separate pools. If not enough space is available, then the file system is not created.</li> </ul>

For example:

```
Storage> tier addmirror fs1 pool5
100% [#] Adding mirror to secondary tier of filesystem
```

### To remove a mirror from a tier of a file system

- ◆ To remove a mirror from a tier of a file system, enter the following:

```
Storage> tier rmmirror fs_name
```

where *fs\_name* specifies the name of the tiered file system from which you want to remove a mirror.

For example:

```
Storage> tier rmmirror fs1
```

This command provides another level of detail for the remove mirror operation. You can use the command to specify which mirror you want to remove by specifying the pool name or disk name.

The disk must be part of a specified pool.

### To remove a mirror from a tier spanning a specified pool or disk

- ◆ To remove a mirror from a tier that spans a specified pool or disk, enter the following:

```
Storage> tier rmmirror fs_name [pool_or_disk_name]
```

*fs\_name* Specifies the name of the file system from which to remove a mirror. If the specified file system does not exist, an error message is displayed.

*pool\_or disk\_name* Specifies the pool or disk from which the mirror of the tiered file system spans.

The syntax for the `Storage> tier rmmirror` command is the same for both pool and disk. If you try to remove a mirror using `Storage> fs rmmirror fs1 abc`, Veritas Access first checks for the pool with the name `abc`, then Veritas Access removes the mirror spanning on that pool. If there is no pool with the name `abc`, then Veritas Access removes the mirror that is on the `abc` disk. If there is no disk with the name `abc`, then an error message is displayed.

## Listing all of the files on the specified tier

You can list all of the files that reside on either the primary tier or the secondary tier.

---

**Note:** If the tier contains a large number of files, it may take some time before the output of this command is displayed.

---

### To list all of the files on the specified tier

- ◆ To list all of the files on the specified tier, enter the following:

```
Storage> tier listfiles fs_name {primary|secondary}
```

where *fs\_name* indicates the name of the tiered file system from which you want to list the files. You can specify to list files from either the primary or the secondary tier.

For example:

```
Storage> tier listfiles fs1 secondary
```

## Displaying a list of SmartTier file systems

You can display a list of SmartTier file systems using the `Storage> fs list` command.

See [“Listing all file systems and associated information”](#) on page 352.

## Displaying the tier location of a specified file

### To display the tier location of a specified file

- ◆ To display the tier location of a specified file, enter the following:

```
Storage> tier mapfile fs_name file_path
```

**fs\_name** Specifies the name of the file system for which the specified file on the tiered file system resides. If the specified file system does not exist, an error message is displayed.

**file\_path** Specifies the tier location of the specified file. The path of the file is relative to the file system.

For example, to show the location of `a.txt`, which is in the root directory of the `fs1` file system, enter the following:

```
tier mapfile fs1 /a.txt
Tier      Extent Type  File Offset  Extent Size
====      =====
Primary   Data          0 Bytes     1.00 KB
```

## About tiering policies

Each tier can be assigned a policy.

The tiering policies include:

- Specify on which tier (primary or secondary) the new files get created.
- Relocate files from the primary tier to the secondary tier based on any number of days of inactivity of a file.
- Relocate files from the secondary tier to the primary tier based on the Access Temperature of the file.
- Prune files on the secondary tier based on the number of days of inactivity of a file.

# About configuring the policy of each tiered file system

You can configure the policy of each tiered file system.

**Table 28-1** Tier policy commands

Command	Definition
tier policy list	<p>Displays the policy for each tiered file system. You can have one policy for each tiered file system.</p> <p>See <a href="#">“Configuring the policy of each tiered file system”</a> on page 486.</p>
tier policy modify	<p>Modifies the policy of a tiered file system.</p> <p>The new files are created on the primary tier. If a file has not been accessed for more than seven days, the files are moved from the primary tier to the secondary tier. If the access temperature is more than five for of the files in the secondary tier, these files are moved from the secondary tier to the primary tier. The access temperature is calculated over a three-day period.</p> <p>See <a href="#">“Configuring the policy of each tiered file system”</a> on page 486.</p>
tier policy prune	<p>Specifies the prune policy of a tiered file system.</p> <p>Once files have aged on the secondary tier, the prune policy can be set up to delete those aged files automatically.</p> <p>The sub-commands under this command are:</p> <ul style="list-style-type: none"> <li>■ tier policy prune list</li> <li>■ tier policy prune modify</li> <li>■ tier policy prune remove</li> </ul> <p>See <a href="#">“Configuring the policy of each tiered file system”</a> on page 486.</p>
tier policy run	<p>Runs the policy of a tiered file system.</p> <p>See <a href="#">“Configuring the policy of each tiered file system”</a> on page 486.</p>
tier policy remove	<p>Removes the policy of a tiered file system.</p> <p>See <a href="#">“Configuring the policy of each tiered file system”</a> on page 486.</p>

# Configuring the policy of each tiered file system

## To display the policy of each tiered file system

- ◆ To display the policy of each tiered file system, enter the following:

```
Storage> tier policy list
```

For example:

```
Storage> tier policy list
FS      Create on  Days  MinAccess Temp  PERIOD
==      =====  ====  =====
fs1     primary    2      3              4
```

Each tiered file system can be assigned a policy. A policy that is assigned to a file system has three parts:

file creation	Specifies on which tier the new files are created.
inactive files	Indicates when a file has to be moved from the primary tier to the secondary tier. For example, if the <code>days</code> option of the tier is set to 10, and if a file has not been accessed for more than 10 days, then it is moved from the primary tier of the file system to the secondary tier.
access temperature	Measures the number of I/O requests to the file during the period as designated by the period. In other words, it is the number of read or write requests that are made to a file over a specified number of 24-hour periods, divided by the number of periods. If the access temperature of a file exceeds <code>minacctemp</code> (where the access temperature is calculated over a period of time previously specified) then this file is moved from the secondary tier to the primary tier.

**To modify the policy of a tiered file system**

- ◆ To modify the policy of a tiered file system, enter the following:

```
Storage> tier policy modify fs_name {primary|secondary} days
minacctemp period
```

fs_name	The name of the tiered file system from which you want to modify a policy.
tier	Causes the new files to be created on the primary or the secondary tier. You need to input either <code>primary</code> or <code>secondary</code> .
days	Number of days from which the inactive files move from the primary to the secondary tier.
minacctemp	The minimum access temperature value for moving files from the secondary to the primary tier.
period	The number of past days used for calculating the access temperature.

For example:

```
Storage> tier policy modify fs1 primary 6 5 3
ACCESS fs SUCCESS V-288-0 Successfully modifies
tiering policy for File system fs1
```

**To display the prune policy of a tiered file system**

- ◆ To display the prune policy of a tiered file system, enter the following:

```
Storage> tier policy prune list
```

For example:

```
Storage> tier policy prune list
FS                Delete After
=====
fs1                200
fs2                disabled
```

By default, the prune policy status of a tiered file system is `disabled`. The `delete_after` indicates the number of days after which the files can be deleted.

### To modify the prune policy of a tiered file system

- ◆ To modify the prune policy of a tiered file system, enter the following:

```
Storage> tier policy prune modify fs_name delete_after
```

*fs\_name*                    Name of the tiered file system from which you want to modify the prune policy.

*delete\_after*            Number of days after which the inactive files are deleted.

For example:

```
Storage> tier policy prune modify fs0 180
You have set the Prune policy to file system , system will automatically
delete the inactive files on secondary tier.
Do you want to continue with setting the Tier Prune policy? (y/n)
Y
ACCESS fs SUCCESS V-288-0 Successfully modified the Prune policy for
File system fs0
```

### To remove the prune policy of a tiered file system

- ◆ To remove the prune policy of a tiered file system, enter the following:

```
Storage> tier policy prune remove fs_name
```

where *fs\_name* is the name of the tiered file system from which you want to remove the prune policy.

For example:

```
Storage> tier policy prune remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed the Prune policy for
File system fs1
```

### To run the policy of a tiered file system

- ◆ To run the policy of a tiered file system, enter the following:

```
Storage> tier policy run fs_name
```

where *fs\_name* indicates the name of the tiered file system for which you want to run a policy.

For example:

```
Storage> tier policy run fs1
ACCESS fs INFO V-288-1221 The command may take some time to execute,
pressing CTRL + C, will abort the command.
ACCESS fs SUCCESS V-288-1275 Successfully ran tiering policy for
File system fs1
```

### To remove the policy of a tiered file system

- ◆ To remove the policy of a tiered file system, enter the following:

```
Storage> tier policy remove fs_name
```

where *fs\_name* indicates the name of the tiered file system from which you want to remove a policy.

For example:

```
Storage> tier policy remove fs1
ACCESS fs SUCCESS V-288-0 Successfully removed
tiering policy for File system fs1
```

You can run the policy of a tiered file system, which would be similar to scheduling a job to run your policies, except in this case running the policy is initiated manually. The `Storage> tier policy run` command moves the older files from the primary tier to the secondary tier, or prunes the inactive files on the secondary tier, according to the policy setting.

## Best practices for setting relocation policies

Consider the following relocation policy. The following clauses for relocating the files are:

- Clause 1: If the files on the primary tier are not accessed for 10 days, relocate the files to the secondary tier.
- Clause 2: If the Access Temperature of the files on the secondary tier is more than 100 in the last 15 days, then relocate the files to the primary tier.

```
Storage> tier policy list
FS                               Create on   Days   MinAccess Temp   PERIOD
=====
non_pgr                          primary     10     100               15
```

Setting such policies where the "PERIOD" is more than the "Days" may result in files moving between the tiers after running the `Storage> tier policy run` command. For example, if a file `a.txt` was being used a lot between 1-5 days, and the number of inputs/outputs rises to 3000. After the fifth day, the file was not used for 10 days and the `Storage> tier policy run` command was issued. The file `a.txt` has the Access Temp as 3000/15, which is equal to 200. As the file has not been used in the last ten days, the file is moved to the secondary tier. If the `Storage> tier policy run` command is run again, the file moves to the primary tier, as the Min Access Temperature is more than 100.

A best practice is to keep the period for calculating the Minimum Access Temperature to lower than the number of days for checking the access age.

## Relocating a file or directory of a tiered file system

The `Storage> tier relocate` command relocates a file or directory from a secondary tier to a primary tier. This command does not relocate the NDS (Named Data Stream) files that also include extended attributes to the primary tier.

---

**Note:** Relocation is not possible if the primary tier of the file system is full. No error message displays.

---

### To relocate a file or directory

- ◆ To relocate a file or directory, enter the following:

```
Storage> tier relocate fs_name dirPath
```

**fs\_name**                    The name of the tiered file system from which you want to relocate a file or directory. The relocation of the file or directory is done from the secondary tier to the primary tier.

**dirPath**                    Enter the relative path of the directory (`dirPath`) you want to relocate. Or enter the relative path of the file (`file_path`) that you want to relocate.

# About configuring schedules for all tiered file systems

The `tier schedule` commands display, modify, and remove the tiered file systems.

**Table 28-2** Tier schedule commands

Command	Definition
<code>tier schedule modify</code>	Modifies the schedule of a tiered file system. See <a href="#">"Configuring schedules for tiered file systems"</a> on page 491.
<code>tier schedule list</code>	Displays the schedules for all tiered file systems. You can have one schedule for each tiered file system. You cannot create a schedule for a non-existent or a non-tiered file system. See <a href="#">"Configuring schedules for tiered file systems"</a> on page 491.
<code>tier schedule remove</code>	Removes the schedule of a tiered file system. See <a href="#">"Configuring schedules for tiered file systems"</a> on page 491.

## Configuring schedules for tiered file systems

### To modify the schedule of a tiered file system

- ◆ To modify the schedule of a tiered file system, enter the following:

```
Storage> tier schedule modify fs_name minute hour  
day_of_the_month month day_of_the_week  
node_name
```

For example, enter the following:

```
Storage> tier schedule modify fs1 1 1 1 * * *  
ACCESS fs SUCCESS V-288-0 Command 'tier schedule modify'  
executed successfully for fs1
```

The default node name is the master node.

---

**Note:** If a previous schedule operation is still running, a new schedule is not created until the previous schedule operation is completed.

---

fs_name	Specifies the file system where the schedule of the tiered file system resides. If the specified file system does not exist, an error message is displayed.
minute	This parameter may contain either an asterisk, (*), which implies "every minute," or a numeric value between 0-59.  You can enter */(0-59), a range such as 23-43, or only the *.
hour	This parameter may contain either an asterisk, (*), which implies "run every hour," or a number value between 0-23.  You can enter */(0-23), a range such as 12-21, or only the *.
day_of_the_month	This parameter may contain either an asterisk, (*), which implies "run every day of the month," or a number value between 1-31.  You can enter */(1-31), a range such as 3-22, or only the *.
month	This parameter may contain either an asterisk, (*), which implies "run every month," or a number value between 1-12.  You can enter */(1-12), a range such as 1-5, or only the *. You can also enter the first three letters of any month (must use lowercase letters).
day_of_the_week	This parameter may contain either an asterisk (*), which implies "run every day of the week," or a numeric value between 0-6. The number 0 is interpreted as Sunday. You can also enter the first three letters of the week (must use lowercase letters).
node_name	Specifies the node on which the schedule of the tiered file system will be run. When creating a schedule for a tiered file system, if you do not input a node name, the schedule will be run on the master node. If you specify a node name, the schedule will be run on the specified node.

**To display schedules for all tiered file systems**

- ◆ To display schedules for all tiered file systems, enter the following:

```
Storage> tier schedule list [fs_name]
```

where *fs\_name* indicates the name of the tiered file system for which you want to run a policy.

For example:

```
Storage> tier schedule list
FS      Minute   Hour   Day   Month   WeekDay  NodeName
===     =====  ====  ===  =====  =====  =====
fs1     1         1     1     *       *         master node
```

**To remove the schedule of a tiered file system**

- ◆ To remove the schedule of a tiered file system, enter the following:

```
Storage> tier schedule remove fs_name
```

where *fs\_name* is the name of the tiered file system from which you want to remove a schedule.

For example:

```
Storage> tier schedule remove fs1
ACCESS fs SUCCESS V-288-0 Command tier schedule remove
executed successfully for fs1
```

## Displaying the files that may be moved or pruned by running a policy

Before a policy runs, you can display a list of the files that the policy may move or prune. This feature is useful as a "what if" type of analysis. The command does not physically move any file blocks.

**Allowing metadata information on the file system to be written on the secondary tier****To display a list of files that may be moved or pruned by running a policy**

- ◆ To display a list of files that may be moved or pruned by running a policy, enter the following:

```
Storage> tier query fs_name
```

where *fs\_name* is the name of the tiered file system for which you want to display the list.

For example:

```
Storage> tier query fs1
```

```
Are you sure, this command may take a long time to execute and  
extensively use the system resources, enter yes/no  
Continuing with the command, you can press CTRL+C to abort  
the command
```

```
Yes
```

```
/a.txt
```

```
/b.txt
```

```
/c.txt
```

```
/d.txt
```

## Allowing metadata information on the file system to be written on the secondary tier

The `Storage> tier allowmetadata yes` command allows the metadata information on the specified file system to be written on the secondary tier as well. By default, the secondary tier is not configured for storing metadata information on the file system. Tiers configured with this option show `metaOK` in the column `SECONDARY TIER` of the `Storage> fs list` command output.

### To allow metadata information on the file system to be written on the secondary tier

- ◆ To allow metadata information on the file system to be written on the secondary tier, enter the following:

```
Storage> tier allowmetadata yes fs_name
```

where *fs\_name* is the name of the file system where metadata information can be written on the secondary tier.

For example:

```
Storage> tier allowmetadata yes fs1  
ACCESS fs SUCCESS V-288-0 Configured the secondary tier for storing  
metadata information.
```

## Restricting metadata information to the primary tier only

The `Storage> tier allowmetadata no` command restricts the metadata information to the primary tier only. If the primary tier gets full, the write operations to the secondary tier are not served as the metadata updates. They are restricted to the primary tier only.

### To restrict metadata information to the primary tier only

- ◆ To restrict metadata information to the primary tier only, enter the following:

```
Storage> tier allowmetadata no fs_name
```

where *fs\_name* is the name of the file system where the metadata information is restricted to the primary tier only.

For example:

```
Storage> tier allowmetadata no fs1  
ACCESS fs SUCCESS V-288-0 Configured the secondary tier for storing  
no metadata information.
```

## Removing a tier from a file system

The `Storage> tier remove` command removes a tier from the file system and releases the storage that is used by the file system back to the storage pool. All

the files on the secondary tier are relocated to the primary tier. The file system must be online when using the `Storage> tier remove` command.

---

**Note:** If the storage tier to be removed contains any data residing on it, then the tier cannot be removed from the file system.

---

---

**Note:** Ensure that you remove the policy first by running the `Storage> tier policy remove` command prior to running the `Storage> tier remove` command.

---

See [“Configuring the policy of each tiered file system”](#) on page 486.

### To remove a tier from a file system

- ◆ To remove a tier from a file system, enter the following:

```
Storage> tier remove fs_name
```

where *fs\_name* specifies the name of the tiered file system that you want to remove.

For example:

```
Storage> tier remove fs1
```

# Configuring cloud as a tier

This chapter includes the following topics:

- [Configuring the cloud as a tier feature for scale-out file systems](#)
- [Moving files between tiers in a scale-out file system](#)
- [About policies for scale-out file systems](#)
- [Obtaining statistics on data usage in the cloud tier in scale-out file systems](#)

## Configuring the cloud as a tier feature for scale-out file systems

You can move data to the Amazon S3 cloud using a tiering mechanism if you use a scale-out file system. A cloud container is used as a storage tier in a scale-out file system. The terms cloud container and cloud tier are used interchangeably.

See [“About scale-out file systems”](#) on page 335.

---

**Warning:** When an Amazon S3 account is used as a cloud tier for a 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.

---

See [“Moving files between tiers in a scale-out file system”](#) on page 498.

See the `storage_cloud(1)` man page for detailed examples.

See the `storage_tier(1)` man page for detailed examples.

---

**Warning:** Veritas Access cannot add a cloud tier if the clock on the Veritas Access system is more than 15 minutes out-of-sync with the actual time. To ensure that the Veritas Access clock time is accurate, configure an NTP server or use the `System> clock set` command.

---

See [“Coordinating cluster nodes to work with NTP servers”](#) on page 85.

See [“Setting the system clock”](#) on page 89.

### To configure the cloud as a tier for scale-out file systems

- 1 Display the available cloud services.

```
Storage> cloud listservice service_name
```

If the cloud service is not listed, you may need to add the cloud subscription to the cluster.

See [“About the cloud gateway”](#) on page 138.

- 2 Add the cloud as a tier to a scale-out file system.

```
Storage> tier add cloud fs_name tier_name service_name  
region
```

Amazon AWS has standard regions defined. Based on the region you choose in Veritas Access, AWS storage is served through that region. To get better performance, always select the closest geographic region.

- 3 Verify that the cloud tier is configured on the specified scale-out file system.

```
Storage> tier list fs_name
```

### To remove the cloud tier

- ◆ Remove the cloud tier.

```
Storage> tier remove fs_name tier_name
```

If there are any files present in the cloud tier, the remove cloud tier operation fails. Move the files back to the primary tier before removing the cloud tier.

## Moving files between tiers in a scale-out file system

By default, a scale-out file system has a single primary tier, which is the on-premises storage for the scale-out file system. You can add a cloud service as an additional

tier. After a cloud tier is configured, you can move data between the tiers of the scale-out file system as needed.

Use the commands in this section to move data as a one-time operation. For example, if you have just set up a cloud tier, and you want to move some older data to that tier.

If you want to specify repeatable rules for maintaining data on the tiers, you can set up a policy for the file system.

You can specify the following criteria to indicate which files or directories to move between tiers:

- file or directory name pattern to match
- last accessed time (`atime`)
- last modified time (`mtime`)

Because a scale-out file system can be large, and the size of the files to be moved can be large as well, the `Storage> tier move` command lets you perform a dry run.

See the `storage_tier(1)` man page.

### To move data between storage tiers in a scale-out file system

- 1 (Optional) Perform a dry run to see which files would be moved and some statistics about the move.

```
Storage> tier move dryrun fs_name source_tier destination_tier pattern  
[atime condition] [mtime condition]
```

The dry run starts in the background. The command output shows the job ID.

- 2 Move the files that match *pattern* from *source\_tier* to *destination\_tier* based on the last accessed time (*atime*) or the last modified time (*mtime*).

```
Storage> tier move start fs_name source_tier destination_tier pattern
[atime condition] [mtime condition]
```

*pattern* is required. To include all the files, specify \* for *pattern*.

The *condition* for *atime* or *mtime* includes an operator, a value, and a unit. Possible operators are the following: <, <=, >, >=. Possible units are m, h, and d, indicating minutes, hours, and days.

The name of the default tier is *primary*. The name of the cloud tier is specified when you add the tier to the file system.

The move job starts in the background. The command output shows the job ID.

Examples:

Move the files that match *pattern* and that have not been accessed within the past 100 days to the cloud tier.

```
Storage> tier move start lfs1 primary cloudtier1 pattern
atime >100d
```

Move the files that match *pattern* and that have been accessed recently in the past 30 days to the specified tier.

```
Storage> tier move start lfs1 cloud_tier primary pattern atime <=30d
```

Move the files that match *pattern* and that have not been modified within the past 100 days to the cloud tier.

```
Storage> tier move start lfs1 primary cloud_tier pattern
mtime >=100d
```

Move only the files that match *pattern* and that were modified within the last three days from the cloud tier to the primary tier.

```
Storage> tier move start lfs2 cloud_tier primary pattern mtime >=3d
```

Move all files to the primary tier.

```
Storage> tier move start lfs2 cloud_tier primary *
```

- 3 View the move jobs that are in progress in the background. This command lists the job IDs and the status of the job.

```
Storage> tier move list
```

Job	Fs name	Source Tier	Destination Tier	Pattern	Atime	Mtime	State
1473684478	largefs1	cloudtier	primary	/vx/largefs1/*	>120s	-	not running
1473684602	largefs1	cloudtier	primary	/vx/largefs1/*	-	-	scanning

- 4 View the detailed status of the data movement for the specified job ID.

```
Storage> tier move status jobid
```

For example:

```
Storage> tier move status 1473682883
```

```
Job run type:      normal
Job Status:       running
Total Data (Files): 4.0 G (100)
Moved Data (Files): 100.0 M (10)
Last file visited: /vx/fstfs/10.txt
```

- 5 If required, you can abort a move job.

```
Storage> tier move abort jobid
```

## About policies for scale-out file systems

When a scale-out file system includes a cloud tier, you can use policies to control the movement of data between the on-premises storage and the cloud tier. A policy is a set of rules defined for a file system for deleting data or moving data. If you want to specify repeatable rules for maintaining data on the tiers, you can set up a policy for the file system.

Each rule defines the following criteria:

- what action should be taken (move or delete)
- when the data should be moved or deleted based on the access time or modified time of the file
- which data should be moved based on the pattern matching for the files and directories.

See [“About pattern matching for data movement policies”](#) on page 503.

Each file system can have more than one rule, though you should be careful not to create rules that conflict or cause looping.

To move or delete the data, you run the policy. When you run a policy, the rules are applied to the data at the time the policy is run. The policy does not run automatically. You can attach a schedule to a policy to have it run automatically at the specified times.

See “[Creating and scheduling a policy for a scale-out file system](#)” on page 505.

## About pattern matching for data movement policies

Within a policy, you can use a pattern to specify that the rule applies to file names or directory names that match the pattern. By using a pattern, you do not need to know the exact file name in advance; the files that match the pattern are selected dynamically.

A pattern uses special characters, which are case sensitive. There are the following types of patterns:

- Directory patterns  
A pattern that ends with a slash (/) is matched only against directories.
- File patterns  
A pattern that does not end with a slash (/) is matched only against files.

The following is a list of supported special characters and their meanings:

* (asterisk)	Matches any character any number of times.
? (question mark)	Matches any single character.
** (two asterisks)	Matches across child directories recursively.  The pattern <code>fs1/**/*.pdf</code> will match <code>.pdf</code> file names present after first sub-directory of <code>fs1/</code> . For example, if the following files exist:  <code>fs1/dir1/a.pdf</code> <code>fs1/dir2/b.pdf</code> <code>fs1/dir3/dir4/c.pdf</code>  then the pattern <code>fs1/**/*.pdf</code> will match only <code>a.pdf</code> and <code>b.pdf</code> . It will not match <code>c.pdf</code> .  The pattern <code>fs1/**/*.pdf</code> will match <code>.pdf</code> files in any directory after <code>fs1</code> . For the above file list, it will match all of the files: <code>a.pdf</code> , <code>b.pdf</code> , and <code>c.pdf</code> .

[ ] (square brackets)	Matches either range or set of characters. [0-5] will match any character in range of 0 to 5. [a-g] will match any character in range of a to g. [abxyz] will match any one character out of a,b,x,y,z.
! (exclamation point)	Can be used as the first character in a range to invert the meaning of the match. ![0-5] will match any character which is not in range of 0 to 5.
\ (backslash)	Can be used as an escape character. Use this to match for one of the above pattern matching characters to avoid the special meaning of the character.

## About schedules for running policies

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 lower case 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 lower case 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
```

## Creating and scheduling a policy for a scale-out file system

By default, a scale-out file system has a single disk tier, which is the on-premises storage for the scale-out file system. You can add a cloud service as an additional tier. After a cloud tier is configured, you can move data between the tiers of the scale-out file system as needed.

Use policies to define a set of data movement rules for the scale-out file system. Each file system can include a policy for deletion and a policy for data movement between tiers.

Be careful when specifying the criteria for moving files. Conflicting policies may cause data to move from one tier to another tier. A best practice is to use policies with a smaller data set first before applying those policies to file systems using a schedule.

A data movement policy can use the following criteria to indicate which files or directories to move between tiers:

- pattern
- atime
- mtime

You can also perform a dry run of a policy.

See the `storage_fs(1)` man page for detailed examples.

## To create a policy

- 1 View the policies that are associated with the file system.

```
Storage> fs policy list fs_name
```

- 2 Create a move policy or a delete policy.

For a move policy:

```
Storage> fs policy add policy_name fs_name operation=move  
from_tier to_tier pattern {atime|mtime}
```

For a delete policy:

```
Storage> fs policy add policy_name fs_name operation=delete from_tier  
pattern {atime|mtime}
```

- 3 If you want to test the policy, you can perform a dry run:

```
Storage> fs policy dryrun policy_name
```

- 4 To move or delete the files according to the policy, run the policy manually or attach a schedule to the policy.

To run the policy manually:

```
Storage> fs policy run policy_name
```

To attach a schedule to the policy:

```
Storage> fs policy schedule create fs_name minute hour day_of_the_month  
month day_of_the_week
```

- 5 Check on the status of the currently running policy or dry run of the policy.

```
Storage> fs policy status
```

- 6 If necessary, you can abort a policy.

```
Storage> fs policy abort
```

# Obtaining statistics on data usage in the cloud tier in scale-out file systems

You can find the following information for data stored in the cloud tier in a scale-out file system:

- Storage utilization in the cloud
- Number of the objects that are stored in the cloud  
See [“Creating buckets and objects”](#) on page 237.
- Number of the files that are stored in the cloud
- Number of GET, PUT, and DELETE requests

See the `storage_tier(1)` man page for detailed examples.

## To display the number of GET, PUT, and DELETE requests

- ◆ Show the number of GET (read requests), PUT (update or replacement requests), and DELETE (deletion requests).

```
Storage> tier stats show fs_name tier_name
```

These statistics are maintained in memory and so are not persistent across reboots.

Example:

```
Storage> tier stats show largefs1 cloudtier
GET          168
GET bytes   174.5MB
PUT          918
PUT bytes   10.3GB
DELETE       20
```

### To monitor the usage of data in the cloud tier

- ◆ Monitor the usage of data in the cloud tier.

```
Storage> tier stats monitor fs_name tier_name [interval]
```

Example:

```
Storage> tier stats monitor largefs1 cloudtier
GET      GET bytes      PUT      PUT bytes      DELETE
6        384.0MB        4        256.0MB        6
0         0              0         0              0
0         0              0         0              0
0         0              2        128.0MB        0
0         0              0         0              0
```

The default interval is five seconds.

### To show the total data usage in the cloud tier

- ◆ Show the total data usage in the cloud tier.

```
Storage> tier stats usage fs_name tier_name
```

Unlike the `Storage> tier stats show` command, these statistics are persistent across reboots.

Example:

```
Storage> tier stats usage largefs1 cloudtier
Storage Utilized  223.1GB
Number of objects 488
Number of files   231
```

This example shows that 223.1 GB is used in the cloud tier. Based on the size of the file, each file is chunked to multiple objects when moved to the cloud, so 231 files were stored as 488 objects in the cloud.

### To reset the in-memory statistics of the cloud tier to zero

- ◆ Reset the statistics of the specified cloud tier to zero.

```
Storage> tier stats reset fs_name tier_name
```

After executing the `Storage> tier stats reset` command, the output for the `Storage> tier stats show` command is reset to zero.

# Configuring SmartIO

This chapter includes the following topics:

- [About SmartIO for solid-state drives](#)
- [About SmartIO read caching for applications running on Veritas Access file systems](#)
- [Setting up SmartIO read caching for Veritas Access](#)
- [About SmartIO writeback caching for applications running on Veritas Access file systems](#)
- [Setting up SmartIO writeback caching for VxFS file systems](#)
- [Customizing the caching behavior](#)
- [Tuning the writeback caching](#)
- [Verifying the VxFS cache area and monitoring the caching](#)
- [Viewing the caching statistics for a cache area](#)
- [Flushing dirty data from a writeback cache area](#)
- [Setting the caching mode](#)

## About SmartIO for solid-state drives

Solid-state drives (SSDs) are devices that do not have spinning disks. Today's solid-state technologies, such as DRAM and NAND flash, provide faster data access, are more efficient, and have a smaller footprint than traditional spinning disks. The data center uses solid-state technologies in many form factors: in-server, all flash arrays, all flash appliances, and mixed with traditional HDD arrays. Each form factor offers a different value proposition. SSDs also have many connectivity types: PCIe, FC, SATA, and SAS.

**About SmartIO read caching for applications running on Veritas Access file systems**

Due to the current cost per gigabyte of SSD devices, the best value of SSDs is not as high capacity storage devices. The benefit of adopting SSDs is to improve performance and reduce the cost per I/O per second (IOPS). Data efficiency and placement is critical to maximizing the returns on any data center's investment in solid state.

The SmartIO feature of Veritas Access enables data efficiency on your SSDs through I/O caching. Using SmartIO to improve efficiency, you can optimize the cost per IOPS. SmartIO does not require in-depth knowledge of the hardware technologies underneath. SmartIO uses advanced, customizable heuristics to determine what data to cache and how that data gets removed from the cache. The heuristics take advantage of Veritas Access' knowledge of the characteristics of the workload.

SmartIO uses a cache area on the target device or devices. The cache area is the storage space that SmartIO uses to store the cached data and the metadata about the cached data. To start using SmartIO, you can create a cache area with a single command, while the application is online.

When the application issues an I/O request, SmartIO checks to see if the I/O can be serviced from the cache. As applications access data from the underlying volumes or file systems, certain data is moved to the cache based on the internal heuristics. Subsequent I/Os are processed from the cache.

SmartIO supports read and write caching for the VxFS file systems that are mounted on VxVM volumes, in several caching modes and configurations.

See [“About SmartIO read caching for applications running on Veritas Access file systems”](#) on page 510.

See [“About SmartIO writeback caching for applications running on Veritas Access file systems ”](#) on page 512.

## About SmartIO read caching for applications running on Veritas Access file systems

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.

## Setting up SmartIO read caching for Veritas Access

In read mode, the SmartIO feature caches the file system read I/Os. To set up SmartIO for read caching for a file system, simply create the cache area.

### Setting up SmartIO read caching

- 1 For each node, to view a list of devices available to use for the SmartIO cache area, use the following command:

```
SMARTIO> device list node_name
```

Where:

*node\_name* specifies the cluster node.

- 2 Create the cache area on the SSD device, using the following command.

```
SMARTIO> cache create node_name device_name
```

Where:

*node\_name* specifies the cluster node on which to create the SmartIO cache.

*device\_name* specifies a device to use for the cache area.

For example:

```
SMARTIO> cache create access1_01 sdb
```

### 3 The cache area is set to read mode by default.

When a cache area is deleted or brought offline, the caching mode is not removed from the file system mount options. If you create or bring online a new cache area, the cache area inherits the existing caching mode.

If the file system mount option was previously set to writeback, you must explicitly change the caching mode as follows:

```
SmartIO> fs cachemode read fs_name
```

For example:

```
SmartIO> fs cachemode read target1
Cluster-configuration updated with changed
Mount Options for node access1_01
Mount Point /vx/target1 remounted successfully on access1_01
```

### 4 If required, you can further customize the caching behavior.

See [“Customizing the caching behavior”](#) on page 514.

## About SmartIO writeback caching for applications running on Veritas Access file systems

Veritas Access supports writeback caching on solid-state drives (SSDs) for applications running on Veritas Access file systems. In this scenario, application reads and writes are satisfied from the cache whenever possible.

SmartIO provides write caching in the writeback mode. 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. Write order fidelity is not guaranteed while flushing the dirty data to the disk.

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. Veritas Access provides additional protection from data loss with cache reflection. Cache reflection is enabled by default.

Writeback caching requires a cluster with exactly two nodes. Writeback caching cannot be enabled if the cluster has more than two nodes or if the cluster has a single node.

When writeback caching is enabled, SmartIO mirrors the writeback data at the file system level to the other node's SSD cache. This behavior, called cache reflection, prevents loss of writeback data if a node fails. If a node fails, the other node flushes the mirrored dirty data of the lost node as part of reconfiguration. Cache reflection ensures that writeback data is not lost even if a node fails with pending dirty data.

After writeback caching is enabled on the mount point, the qualified synchronous writes in that file system are cached. SmartIO determines if a write qualifies for writeback caching, using criteria such as the following:

- The write request must be PAGESIZE aligned (multiple of 4 KB).
- The write request is not greater than 2 MB.
- The file on which the writes are happening is not mapped.
- Writeback caching is not explicitly disabled by the administrator.
- Writeback caching is not qualified if the cluster has more than two nodes.

You can also customize which data is cached, by adding advisory information to assist the SmartIO feature in making those determinations.

## Setting up SmartIO writeback caching for VxFS file systems

In writeback mode, the SmartIO feature caches the VxFS file system read and write I/Os. To set up SmartIO for writeback caching for a VxFS file system, create the cache area and set the caching mode to writeback mode.

Writeback caching requires a cluster with exactly two nodes.

### To set up SmartIO writeback caching for VxFS file systems

- 1 For each node, to view a list of devices available to use for the SmartIO cache area, use the following command:

```
SMARTIO> device list node_name
```

Where:

*node\_name* specifies the cluster node.

- 2 Create the VxFS cache area on the SSD device, using the following command.

```
SMARTIO> cache create node_name device_name
```

Where:

*node\_name* specifies the cluster node on which to create the SmartIO cache.

*device\_name* specifies a device to use for the cache area.

For example:

```
SMARTIO> cache create sfnas1_01 sdb
```

- 3 Set the caching mode for the file system to writeback, using the following command.

```
SmartIO> fs cachemode writeback fs_name
```

For example:

```
SmartIO> fs cachemode writeback target1
```

```
Cluster-configuration updated with changed
```

```
Mount Options for node sfnas1_01
```

```
Mount Point /vx/target1 remounted successfully on sfnas1_01
```

- 4 If required, you can further customize the caching behavior.

See [“Customizing the caching behavior”](#) on page 514.

See [“Tuning the writeback caching”](#) on page 516.

## Customizing the caching behavior

By default, SmartIO caches the file data based on the workload. SmartIO loads portions of files into the cache based on I/O access. When the cache area fills, data may be evicted to make room for caching new data. SmartIO uses criteria such as frequency of access to evict data. While the data is in the cache, the subsequent

I/Os to that file data are satisfied from the cache. If the data is evicted, any subsequent I/O request is served from the primary storage. SmartIO may then cache the data again.

To maximize the use of the cache, you can customize the caching behavior to control when files are loaded or evicted from the cache. You can customize the caching behavior, using the following operations:

- The `load` operation preloads files into the cache before the I/O accesses the files. The files are already in the cache so that the I/Os return more quickly. The files are loaded asynchronously in the background.
- The `pin` operation prevents the files from being evicted from the cache. You can pin commonly used files so that SmartIO does not evict the files and later need to cache the files again. A pinned file is kept in the cache indefinitely, until it is deleted or explicitly unpinned.
- The `unpin` operation removes files from the pinned state. The `unpin` operation does not cause the file to be immediately evicted. SmartIO considers the file for eviction in the same way as any other file, when space is required in the cache.

For each of these operations, you can specify files individually, or specify a directory name to affect all of the files in a directory.

### To load a file or directory

- ◆ To load a file or directory to the cache, specify the file name or the directory name to the following command.

```
SmartIO> file load {file|dir}
```

Where:

*file* is the full path name of the file to be loaded.

*dir* is the directory name. If you specify a directory name, all of the files in the directory are loaded.

For example:

```
SmartIO> file load /vx/target1/demo1.f
```

### To pin a file or directory

- ◆ To pin a file or directory to the cache, specify the file name or directory name to the following command.

```
SmartIO> file pin {file|dir}
```

Where:

*file* is the full path name of the file to be pinned.

*dir* is the directory name. If you specify a directory name, all of the files in the directory are pinned.

For example:

```
SmartIO> file pin /vx/target1/demo1.f
```

### To unpin a file or directory

- ◆ To unpin a file or directory to the cache, specify the file name to the following command.

```
SmartIO> file unpin {file|dir}
```

Where:

*file* is the full path name of the file to be unpinned.

*dir* is the directory name. If you specify a directory name, all of the files in the directory are unpinned.

For example:

```
SmartIO> file unpin /vx/target1/demo1.f
```

## Tuning the writeback caching

When writeback caching is enabled, any data that is read from the disk is cached, unless the file is explicitly marked for "no caching" or if the cache is full. For writes, certain writes cause the data to be cached. You can load a file to speed up the application. Pinning a file in the cache ensures that the data does not get evicted. If some data is already cached, and that portion of the disk is overwritten, then SmartIO also writes the new data to the cache device to ensure that the cached data remains up to date.

You can use the following tunable parameters to adjust the size of the cache and how long data is held in the cache.

### Setting the maximum space used for dirty data per node

## Setting the maximum space used for dirty data per node

When writeback is enabled, you can configure a maximum for the space used for dirty data per node. By default, there is no maximum. If you configure a maximum, you must allow at least 512 MB for each file system or cluster file system. For a cluster file system, the space required for data reflection is not included in the maximum.

### To set the writeback size

- 1 Run the following command to configure the maximum. For a cluster file system, run the command on each node of the cluster to make the setting cluster wide.

```
SMARTIO> cache wb_size=size
```

For example:

```
SMARTIO> cache wb_size=1g
```

- 2 For the changed value to take affect, run the following command.

```
SMARTIO> fs enable target1
```

- 3 The writeback size is shown as Writeback Cache Use Limit, when you display the cache statistics. To display the cache statistics:

```
SMARTIO> cache stat
```

See [“Viewing the caching statistics for a cache area ”](#) on page 518.

# Verifying the VxFS cache area and monitoring the caching

After the SmartIO feature is configured, you can verify that the cache area is present and that caching is occurring.

**To verify and monitor the cache area**

- 1** Use the following command to display information about the cache areas on the system.

```
SmartIO> cache list

NAME           TYPE SIZE  ASSOC-TYPE  STATE  DEVICE
sfcachearea_1 VxFS 7.97g AUTO          ONLINE  sdb
```

- 2** To display information about a specific file:

```
SmartIO> file list target1

/vx/target1:
READ CACHE      WRITEBACK      MODE      PINNED  NAME
    39.0 MB           0 KB      read      yes     /vx/target1
```

- 3** To see statistics on the cache usage, use the following command:

```
SmartIO> fs stat target1

Cache Size:      7.97 GB
Cache Utilization:  1 GB ( 12.56 %)

Read Cache
Hit Ratio      Data Read      Data Written

/vx/target1:
    0.00 %           0 KB           0 KB
```

The output displays statistics for the cached data.

See [“Viewing the caching statistics for a cache area”](#) on page 518.

## Viewing the caching statistics for a cache area

For a VxFS cache area, the statistics do not change after you unmount and mount the file systems. For a cluster file system, the statistics do not change after you reboot the cluster nodes.

**To view the caching statistics for a VxFS cache area**

- ◆ Use the following command:

```
SMARTIO> cache stat
```

```
TYPE: VxFS
NAME: sfcachearea_1
      Cache Size:      7.97 GB
      Cache Utilization: 18.66 MB (.23 %)
File Systems Using Cache:      2
Writeback Cache Use Limit: Unlimited
Writeback Flush Timelag:      10 s
```

Read Cache		Writeback		
Hit Ratio	Data Read	Data Written	Hit Ratio	Data Written
Total:				
0.00 %	0 KB	195.0 MB	100.00 %	78.0 MB
/target1:				
0.00 %	0 KB	78.0 MB	100.00 %	39.0 MB
/shared:				
0.00 %	0 KB	39.0 MB	0.00 %	0 KB

## Flushing dirty data from a writeback cache area

With SmartIO, dirty data in the cache is automatically flushed to the disk during normal operations. The dirty data is flushed when the file system is unmounted, or during other operations that require a file system freeze. The dirty data is also flushed periodically at intervals. You can control the interval by configuring the tunable parameters.

See [“Tuning the writeback caching”](#) on page 516.

Disabling writeback caching for a file also flushes any writeback dirty data for that file.

In some cases, you may want to manually trigger flushing of the dirty data from the cache to the disk. For example, to ensure data consistency, you would flush the cache before you create an array level snapshot.

You can manually trigger flushing of the dirty data using the following command.

```
SmartIO> fs flush target1
```

## Setting the caching mode

You can set the caching mode of a file system. For a VxFS cache area, the caching mode determines what kind of caching is performed for the specified mount point. The mode can be `nocache`, `read`, or `writeback`. The default mode is `read`.

When a cache area is deleted or brought offline, the caching mode of the cache area is not changed. If you create or bring online a new cache area, the cache area inherits the existing caching mode. If a different caching mode is required, you must explicitly change the caching mode.

### To change the caching mode of a file system

- ◆ To change the caching mode of a file system, use the following command.

```
SmartIO> fs cachemode {nocache|read|writeback} file system
```

For example:

```
SmartIO> fs cachemode writeback target1
```

```
Cluster-configuration updated with changed
```

```
Mount Options for node sfnas1_01
```

```
Mount Point /vx/target1 remounted successfully on sfnas1_01
```

# Setting up Veritas Access Replication between two clusters

This chapter includes the following topics:

- [About Veritas Access file-level replication](#)
- [How Veritas Access Replication works](#)
- [Accessing the Veritas Access Replication commands](#)
- [Starting Veritas Access Replication](#)
- [Setting up communication between the source and the destination clusters](#)
- [Managing bandwidth limits for Veritas Access replication](#)
- [Setting up the file systems to replicate](#)
- [Setting up files to exclude from a replication unit](#)
- [Scheduling the replication](#)
- [Defining what to replicate](#)
- [About the maximum number of parallel replication jobs](#)
- [Managing a replication job](#)
- [Replicating compressed data](#)
- [Displaying replication job information and status](#)
- [Synchronizing a replication job](#)

- [Behavior of the file systems on the replication destination target](#)
- [Accessing file systems configured as replication destinations](#)
- [Creating a recovery point objective \(RPO\) report](#)
- [Replication job failover and failback](#)

## About Veritas Access file-level replication

The Veritas Access Replication solution provides high performance, scalable (one-to-many) data replication and is ideal for use as a content distribution solution, and for use to create hot standby copies of important data sets.

Veritas Access Replication lets you asynchronously replicate a file system from one node in a source cluster to another node in a destination cluster at regularly timed intervals. This allows for content sharing, replication, and distribution.

The Veritas Access Replication functionality allows episodic replication with a minimum timed interval update of 15 minutes and no set maximum. Unlike many replication solutions, Veritas Access Replication also allows the destination file system to be online for reads while replication is active.

Major features of Veritas Access Replication include:

- Online access (read-only) to replicated data.
- Immediate read/write access to destination replicated data in the unlikely event that the source file system goes offline for a sustained period of time.
- Load balancing across replication links.
- Transport failover of replication service from one node to another.
- Unlimited simultaneous replication operations.

The Veritas Access Replication feature is designed to copy file systems only between Veritas Access clusters.

---

**Note:** The Veritas Access Replication feature does not support user modifications to the target file system if replication is configured.

---

You can manage bandwidth during replication by actively manage bandwidth using the bandwidth limit throttle.

See [“Managing bandwidth limits for Veritas Access replication”](#) on page 538.

You can perform Veritas Access Replication operations from the Veritas Access CLI.

## How Veritas Access Replication works

Veritas Access Replication is an incremental file-level replication service that runs on top of the Cluster File System that is used by Veritas Access which is, in turn, based on the Veritas File System (VxFS). Veritas Access Replication uses two file system specific features: File Change Log (FCL) and Storage Checkpoint services, to retrieve file changes between replication periods.

For a given period, the FCL records every change made to the file system. By scanning the FCL, Veritas Access Replication quickly identifies the file(s) that have changed and generates the modified file list. This avoids the expensive file system scanning that is normally associated with file-based replication, and which typically results in sub-optimal performance.

Next, Veritas Access Replication uses VxFS Storage Checkpoint's metadata comparison feature to retrieve the modified extent list of each changed file. It does not need to access the file data.

The Veritas Access Replication transport layer works in conjunction with, and interfaces to the well-known rsync remote file synchronization tool. Using this existing network transportation program makes the network configuration much easier in the enterprise domain: the Secure Socket Shell (SSH) port (22) required by rsync is opened by default on almost all enterprise firewalls. rsync is also a reliable solution for a low bandwidth or unreliable link environment.

---

**Note:** Veritas Access uses the rsync protocol to provide transportation of Veritas Access Replication encapsulated files. The use of rsync is not exposed in Veritas Access, and cannot be administered outside of the Veritas Access Replication feature set.

---

## Accessing the Veritas Access Replication commands

This chapter describes how to set up, configure, and enable Veritas Access Replication between two Veritas Access clusters.

You run Veritas Access Replication between two Veritas Access clusters which are referred to as the source cluster and the destination cluster.

source                      The source is where the data is replicated from.

destination                The destination is where the data is replicated to.

Veritas Access Replication requires communication between both clusters. This communication occurs over TCP/IP Port 22 (SSH) so ensure that port 22 is open across the network between the two clusters.

---

**Note:** The source and destination virtual IP addresses being used for replication between clusters must have port 22 access open between the source and destination.

---

---

**Note:** You can confirm if the SSH port is open using the `telnet destination IP SSH port` command.

---

To access the Veritas Access Replication commands, log into your administrative console (master, system-admin, or storage-admin) and enter `Replication>` mode.

Before using the Veritas Access Replication commands, make sure that the source and the destination clusters can communicate with each other over the network.

The most common, and easiest way to verify communication, is to use the `Network> ping` command in the Veritas Access CLI.

## Starting Veritas Access Replication

This section lists the specific commands that are needed to run Veritas Access Replication on your clusters.

---

**Note:** Before you set up your clusters for replication, you must first identify which is the source cluster and which is the destination cluster. All of the commands are performed on the source cluster first.

---

---

**Note:** Make sure both the source cluster and the destination cluster have the same version of Veritas Access.

---

To use Veritas Access Replication, you must first create an online file system on the Veritas Access source cluster and an online file system on the Veritas Access destination cluster.

---

**Note:** Assign a virtual IP (VIP) address to both the source and the destination clusters. The Veritas Access Replication service requires VIP addresses not already in use for the two clusters to communicate.

---

## To start Veritas Access Replication on the source cluster

- 1 To bind a virtual IP address for the replication service on the source cluster, enter the following:

```
Replication> config bind ip_addr [device] [netmask]
```

*ip\_addr* Virtual IP address for the replication service on the source cluster.

*device* The public network interface name that you want the replication IP address to use.

*netmask* Netmask for the replication IP address.

For example:

```
Replication> config bind 10.10.10.10
```

```
Please wait...
```

```
ACCESS replication SUCCESS V-288-0 10.10.10.10 configured as Virtual IP.
```

```
ACCESS replication SUCCESS V-288-0 IP bind completed
```

- 2 To start the replication service, enter the following on the source node:

```
Replication> service start [nodename]
```

*nodename* The name of the node in the local cluster where you want to start the replication service.

For example:

```
Replication> service start
```

```
Starting replication service on ACCESS_01. Please wait...
```

```
ACCESS replication SUCCESS V-288-0 Replication service started
```

```
Replication>
```

- 3** To check the status of the replication service, enter the following:

```
Replication> service status
```

For example:

```
Replication> service status  
Status : RUNNING  
Online On Node : ACCESS_01  
Replication>
```

- 4** To confirm the IP address is up and running, enter the following:

```
Replication> config show ip
```

For example:

```
Replication> config show ip  
Local cluster details:  
=====
```

Replication VIP	: 10.10.10.10
Replication Device	: pubeth0
Online On Node	: ACCESS_01

The definitions of the headings are as follows:

Replication VIP      Virtual IP address for the replication service.

Replication Device    Device that the replication service currently uses.

Online on Node        Cluster node on which the replication service is currently running.

---

**Note:** Alternately, you can use the `network> ip addr show` command to confirm that the IP address is up and running.

---

## To start Veritas Access Replication on the destination cluster

- 1 To bind a virtual IP address for the replication service on the destination cluster, enter the following:

```
Replication> config bind ip_addr [device] [netmask]
```

*ip\_addr* Virtual IP address for the replication service on the source cluster.

*device* The public network interface name that you want the replication IP address to use.

*netmask* Netmask for the replication IP address.

For example:

```
Replication> config bind 10.10.20.20  
Please wait...  
ACCESS replication SUCCESS V-288-0 10.10.20.20 configured as Virtual IP.  
ACCESS replication SUCCESS V-288-0 IP bind completed
```

- 2 To start the replication service, enter the following on the destination node:

```
Replication> service start [nodename]
```

*nodename* The name of the node in the local cluster where you want to start the replication service.

For example:

```
Replication> service start  
Starting replication service on ACCESS_01. Please wait...  
ACCESS replication SUCCESS V-288-0 Replication service started  
Replication>
```

- 3 To check the status of the replication service, enter the following:

```
Replication> service status
```

For example:

```
Replication> service status
Status : RUNNING
Online On Node : ACCESS_01
Replication>
```

- 4 To confirm that the IP address is up and running, enter the following:

```
Replication> config show ip
```

For example:

```
Replication> config show ip
Local cluster details:
=====
Replication VIP      : 10.10.20.20
Replication Device   : pubeth0
Online On Node       : ACCESS_01
```

The definitions of the headings are as follows:

Replication VIP      Virtual IP address for the replication service.

Replication Device    Device that the replication service currently uses.

Online on Node        Cluster node on which the replication service is currently running.

You next need to set up communication between the source and the destination clusters.

See [“Setting up communication between the source and the destination clusters”](#) on page 528.

## Setting up communication between the source and the destination clusters

You need to set up communication between your source and your destination clusters.

Make sure that you already created an online file system on the Veritas Access source cluster and an online file system on the Veritas Access destination cluster.

See “[Starting Veritas Access Replication](#)” on page 524.

Veritas Access Replication authentication strategy is based on RSA-key authentication, and both the source and the destination clusters have to export their replication public keys. The source cluster imports the destination cluster's public key and the destination cluster imports the source cluster's public key.

After you have determined which two Veritas Access clusters to use, you need to authenticate them.

The `Replication> config` commands must be executed in a specific order.

- Use the `Replication> config del_keys` after the `Replication> config deauth` command, or it fails.
- You can only run the `Replication> config unbind` command (to unbind the virtual IP) after you have run the `Replication> service stop` command.
- You need to run the `Replication> config bind` command (to bind the virtual IP) before you can run the `Replication> service start` command.
- You need to run the `Replication> config export_keys` and `Replication> config import_keys` to export and import the keys of both the source and the destination clusters.
- You can only run the `Replication> config auth` command after both the source and destination have imported each others keys.
- You need to run the `Replication> config auth` command to create a link from every cluster to any remaining cluster that is used for replication irrespective of their role as a source or a destination cluster.

After the source and the destination clusters have successfully imported each other's public keys, you need to run the `Replication> config auth` command on the source cluster to complete the authentication between the two clusters. This command checks the two-way communication between the source and the destination clusters, and authenticates the clusters allowing the Veritas Access Replication service to begin.

---

**Note:** The `Replication> config auth` command must be executed from the source cluster.

---

This section provides a walk-through for the creation and export/import of these encrypted keys for both the source and the destination cluster.

In this release of Veritas Access Replication, it is possible to provide a third-party destination to act as an intermediary between nodes for the transfer of the encrypted keys.

---

**Note:** Without the correct authentication of the source and the destination encryption keys, Veritas Access Replication does not function correctly.

---

## To export the source cluster's key to the destination cluster

- 1 To export the source cluster's key to the destination cluster, enter the following:

```
Replication> config export_keys [URL]
```

*URL*                      The location you want to copy the public keys to.

If you do not want to enter a URL, you can copy the output from the

Replication> config export\_keys command into the Replication> config import\_keys command at the destination cluster.

By default, the output is displayed to your computer screen.

The SCP and FTP protocols are supported.

For example, if you entered a URL in the command:

```
Replication> config export_keys scp://username@hostname:~/
Password: *****
ACCESS replication SUCCESS V-288-0
Key file SNASKEY_source_10.10.10.10_2009-05-29
copied successfully at location username@hostname:~/
```

For example, if you did not enter a URL in the command:

```
Replication> config export_keys
Displaying replication key. Please use this key with config
import_keys command.
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEApuUukbe8znGccz9V1UPTwn8JpbtmfQ2eJGQw
Br0IrI6dYyxPVeIb2MhdKjiwwDoHybYkS6YXHR5AFT+m2gocikVYgD1fJppip
6YC1BqTa5h7eII89eRS85PCYwEXhoMJmoUS4cFxzT3gqAMH80eu3aiZHn+
PAU7Tu0xpY1vpTOQ1X661GfbtdLp9ZNF+9qbt/x73yh09HjVCgeTBcMHJZhrbNZ2/
mK7XX8509pM/7yZxSWzCswamuaum3VZBpyX+uwQp/KyvrO5ZnAW5WUO93myqy
ShwJKujRWF02sIm6bvn8pI0ZukMx16etnsLippqttr4ED8SXI1W1A3JysXiXw==
SNAS-replication@source::source_10.209.105.236
```

Config export keys command completed successfully

**2** To import the source cluster's key to the destination cluster, enter the following:

```
Replication> config import_keys [URL/keyfile]
```

*URL*                      The location you want to copy the public keys from.

*keyfile*                 The file name of the key that is generated by the export.

For example:

```
Replication> config import_keys
scp://username@hostname:~/SNASKEY_source_10.209.05.236_2009-05-29
Password: *****
ACCESS replication SUCCESS V-288-1089 Config import keys command
completed successfully
Key file SNASKEY_source_10.10.10.10_2009-05-29
copied successfully at location username@hostname:~/
```

If you did not enter a URL during the `Replication> config export_keys` command, you can cut and paste the output and enter it into the `Replication> config import_keys` command.

For example:

```
Replication> config import_keys
Enter replication key of remote cluster:: ssh-rsa

AAAAB3NzaC1yc2EAAAABIWAAAQEApUukbe8znGccz9V1UPTwn8JpbtnfQ2eJGQw
BrOIrI6dYyxPVeIb2MhdKjiwwDoHybYkS6YXHR5AFT+m2gocIKVYgd1fJppip
6YC1BqTa5h7eII89eRS85PCYwEXhoMJmoUS4cFxzT3gqAMH80eu3aiZHn+
PAU7Tu0xpY1vpTQQ1X661GfbtdLp9ZNF+9qbt/x73yh09HjVCgeTBcMHJZhrbNZ2/
mK7XX8509pM/7yZxSWzCswamuaum3VZBpyX+uwQp/KyvrO5ZnAW5WUO93myqy
ShwJKujRWF02sIm6bvn8pI0ZukMx16etnsLippqttr4ED8SXI1W1A3JysXiXw==
SNAS-replication@source::source_10.209.105.236

Enter console IP address of remote cluster::10.209.105.236
ACCESS replication SUCCESS V-288-1089 Config import keys
command completed successfully
```

- 3** To verify that the key has been imported correctly, enter the following:

```
Replication> config show
```

```
Link name      Remote ConsoleIP  Remote Replication VIP
=====      =====
--           10.209.105.236   --
```

```
Time of Key Import
```

```
=====
Sun Jul 12 04:02:05 UTC 2009
```

```
Time of Authorization
```

```
=====
- _
```

## To export the destination cluster's key to the source cluster

- 1 To export the destination cluster's key to the source cluster, enter the following:

```
Replication> config export_keys [URL]
```

*URL*                      The location you want to copy the public keys to.

The SCP and FTP protocols are supported.

If you do not want to enter a URL, you can cut and paste the output from the `Replication> config export_keys` command to the `Replication> config import_keys` command. By default, the output is displayed to your computer screen.

For example, if you entered a URL with the command:

```
Replication> config export_keys scp://username@hostname:~/
Password: *****
ACCESS replication SUCCESS V-288-0
Key file SNASKEY_destination_10.182.107.133_2009-05-29
copied successfully at location username@hostname:~/
```

For example, if you did not enter a URL with the command:

```
Replication> config export_keys
Displaying replication key. Please use this key with config
import_keys command.
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEApuUkbe8znGccz9V1UPTwn8JpbtnfQ2eJGQw
BrOIrI6dYyxPVeIb2MhdkjiwDoHybYks6YXHR5AFT+m2gocikVYgD1fJppip6Y
C1BqTa5h7eII89eRS85PCYwEXhoMJmoUS4cFxzT3gqAMH80eu3aiZhn+PAU7Tu0
xpY1vpTOQ1X661GfbtdLp9ZNF+9qbt/x73yh09HjVCgeTBcMHJZhrbN22/mK7XX
8509pM/7yZxSWzCswamuauum3VZBpyX+uwQp/KyvrO5ZnAW5WUO93myqyShwJKuj
RWF02sIm6bvn8pI0ZukwMx16etnsLippqttR4ED8SXI1W1A3JysXiXw==
SNAS-replication@source::source_10.182.107.133
```

Config export keys command completed successfully

**2** To import the destination cluster's key to the source cluster, enter the following:

```
Replication> config import_keys [URL/keyfile]
```

*URL*        Enter the URL of the location you want to copy the public keys from.

*keyfile*    Enter the file name of the key that is generated by the export.

For example:

```
Replication> config import_keys
scp://username@hostname:~/SNASKEY_source_10.182.107.133_2009-05-29
Password: *****
ACCESS replication SUCCESS V-288-1089 Config import keys command
completed successfully
Key file SNASKEY_source_10.10.20.20_2009-05-29
copied successfully at location username@hostname:~/
```

If you did not enter a URL during the `Replication> config export_keys` command, you can cut and paste the output and enter it into the `Replication> config import_keys` command.

For example:

```
Replication> config import_keys
Enter replication key of remote cluster:: ssh-rsa

AAAAB3NzaClyc2EAAAABIwAAAQEApuUukbe8znGccz9V1UPTwn8JpbtnfQ2eJGQw
BrOIrI6dYyxPVeIb2MhdkjiwwDoHybYkS6YXHR5AFT+m2gocikVYgD1fJppip
6YC1BqTa5h7eII89eRS85PCYwEXhoMJmoUS4cFxzT3gqAMH80eu3aiZHn+
PAU7Tu0xpY1vpTOQ1X661GfbtdLp9ZNF+9qbt/x73yh09HjVCgeTBcMHJZhrbNZ2/
mK7XX8509pM/7yZxSWzCswamuau3VZBpyX+uwQp/Kyvr05ZnAW5WU093myqy
ShwJKujRWF02sIm6bvn8pI0ZukwMx16etnsLippqttr4ED8SXI1W1A3JysXiXw==
SNAS-replication@destination::destination_10.182.107.133

Enter console IP address of remote cluster::10.182.107.133
ACCESS replication SUCCESS V-288-1089 Config import keys
command completed successfully
```

- 3** To verify that the key has been imported correctly, enter the following:

```
Replication> config show
```

```
Link name      Remote ConsoleIP  Remote Replication VIP  
=====      =====  
--           10.182.107.133   --
```

```
Time of Key Import
```

```
Time of Authorization
```

```
=====  
Sun Jul 12 04:02:05 UTC 2009
```

```
=====  
--
```

**To authenticate source cluster and destination clusters for replication**

- 1 This command should be executed on the source cluster as well as on the destination cluster. To authenticate the public keys on the source cluster and the destination clusters, enter the following:

```
Replication> config auth conIP link_name
```

*conIP* Enter the destination cluster console IP address.

*link\_name* Both the source cluster and the destination cluster need to be assigned a unique identifier (name). This identifier is used to identify the link that is established between the source and the destination clusters. You can use the link name instead of the virtual IP addresses of the source and the destination clusters when using the other replication commands. For example:  
 Pune\_Shanghai.

For example:

```
Replication> config auth 10.182.107.133 dest1
Please wait...
ACCESS replication SUCCESS V-288-0 Config auth command completed
successfully.
```

- 2 To confirm the authentication, enter the following:

```
Replication> config show
Link name      Remote cluster ConsoleIP      Remote cluster Replication IP
=====      =====
dest1         10.182.107.133      10.10.20.20

Time of Key Import          Time of Authorization
=====
Sun Jul 12 04:02:05 UTC 2009      Sun Jul 12 04:02:57 UTC 2009
```

The definitions of the headings when running the `Replication> config show` and `Replication> config show ip` commands are as follows:

- Link name            The name you specified when you ran the `Replication> config auth` command between the local cluster and the remote cluster.
- Remote Console IP    The Management Server console IP address of the remote cluster.

Remote Replication VIP	The replication virtual IP address of the remote cluster.
Time of Key Import	The exact time (in Coordinated Universal Time (UTC) format) you imported the keys of the remote cluster using <code>Replication&gt; config import_keys</code> command.
Time of Authorization	The exact time (in UTC format) you completed the authorization of the remote cluster using the <code>Replication&gt; config auth</code> command.
Replication Device	Device that the replication service uses.
Online on Node	Cluster node on which the replication service is currently running.

---

**Note:** These steps must be executed on every destination side cluster to authenticate the public keys on the source and the destination clusters.

---

Once you have configured the clusters and links, you need to set up the file systems you want to replicate.

See [“Setting up the file systems to replicate”](#) on page 541.

## Managing bandwidth limits for Veritas Access replication

The bandwidth limit throttle command allows administrators to manage bandwidth allocation for replication operations in a way that minimizes the replication impact on other applications.

Unless configured otherwise, Veritas Access replication uses the maximum allowable network bandwidth to replicate data from the primary site to the remote site. If an enterprise uses the same network for other applications, performance declines. The bandwidth limit option throttles a replication task's bandwidth usage to allow other applications to perform smoothly.

The Veritas Access replication bandwidth limit throttles outbound (only) replication traffic. An administrator must set the bandwidth limit for each link in each cluster. When the administrator sets the bandwidth throttle limit on a replication link, all running jobs using that link share the configured bandwidth. The bandwidth throttle does not affect inbound traffic.

The bandwidth limit value for each link is preserved during a cluster configuration export and import. Setting the bandwidth throttle parameter does not require restart of the replication service; changes take place immediately after running the command. The administrator can change the bandwidth limit for any link at any

time, even while the job is running. The new value becomes effective for the currently running jobs.

---

**Note:** For failover, the administrator has the responsibility to set a limit; otherwise it is unlimited.

---

**Note:** The unit for bandwidth limit is in kilobytes per second (KB/s). The `bwlimit set` command fails if the throttle speed is set to less than 0 or more than the maximum speed that is supported by the network interface used by the replication job. If there are multiple jobs using the same target address and port, the `bwlimit set` command sets the throttled bandwidth for all the jobs.

---

### To configure the bandwidth limit throttle

- ◆ To set or modify the bandwidth limit on a given link in a cluster, enter:

```
Replication> bwlimit set link_names limit
```

*link\_names* Specify the name of the replication links for which you want to set the bandwidth limit.

*limit* Specify the throttle speed in KB/s.

For example, to set a bandwidth limit of 50 KB/s on the replication link `pune_cdc` and `pune_mtv`:

```
Replication> bwlimit set pune_cdc,pune_mtv 50
```

The administrator must set the bandwidth limit on each cluster and link; the command cannot be used to set the counter part of a link in a cluster.

### To show bandwidth limit settings

- 1 To display the bandwidth limit settings that are in effect for all replication links, enter:

```
Replication> bwlimit show
```

The output displays the following:

```
Link Name Bandwidth Limit (in KBps)
-----
pune_cdc  20
pune_mtv  50
pune_uk   Unlimited
```

- 2 To display the bandwidth limit settings that are in effect for particular links, enter:

```
Replication> bwlimit show link_names
```

For example:

```
Replication> bwlimit show pune_cdc,pune_mtv
```

The output displays the following:

```
Link Name Bandwidth Limit (in KBps)
-----
pune_cdc  20
pune_mtv  50
```

### To disable the bandwidth limit

- ◆ To disable the bandwidth limit on a given link in a cluster, enter:

```
Replication> bwlimit reset link_names
```

For example:

```
Replication> bwlimit reset pune_cdc
```

If there are multiple jobs using the target IP and port, the bandwidth limit for all the replication jobs is reset.

You can also disable the bandwidth limit on a link by using the `bwlimit set` command and specifying a limit of 0.

# Setting up the file systems to replicate

You need to set up the file systems you want to replicate using the `Replication> repunit` commands. The `Replication> repunit` commands let you define the type of data that you replicate from the source cluster to the destination cluster. All files and folders belonging to a replication unit are replicated together from the source cluster to the destination cluster.

---

**Note:** The maximum number of replication units supported in Veritas Access Replication is 128.

---

Make sure that you already set up communication between your source and the destination clusters.

See [“Setting up communication between the source and the destination clusters”](#) on page 528.

A single replication unit can span across multiple directories and multiple file systems.

A replication unit is defined as an ordered set of entries, where each entry is one of the following:

- A single file system
- A single subdirectory
- A single file
- A pattern entry

---

**Note:** The replication source has to be one of the entry types shown. It cannot be a snapshot or a Storage Checkpoint (ckpt).

---

Veritas Access Replication requires that the source and the destination replication units of a job definition have the same type of ordered entries, that is, every entry pair (one entry from the source and one entry from the destination replication unit) must be of a similar type.

Both can be files, or both can be directories, as shown in the following example:

Replication unit Name	Replication unit Entries
=====	=====
ru1	fs1, fs2/dir1, fs2/f1
ru2	fs4, fs6/dir2, fs5/f2

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. Appending a slash followed by two asterisks '/'\*\*' at the end of a path indicates that it is a directory, and all the contents of the directory are replicated. Member entries are ordered inside a replication unit and such ordering information is used to determine the replication entity pair mapping from the source replication unit to the destination replication unit.

---

**Note:** Make sure that the paths in the destination replication unit exist in the destination cluster.

---

---

**Note:** The commands in this section apply only to the source replication unit.

---

**To create a replication unit**

- 1 From the source cluster, to create a replication unit, enter the following:

```
Replication> repunit create repunit_name
    repunit_entry[,repunit_entry,...]
```

*repunit\_name*      The name of the replication unit you want to create.

*repunit\_entry*     The file system file, file, folder, or directory.

For example:

```
Replication> repunit create ru3 fs1/dir1,fs2/dir2
ACCESS replication SUCCESS V-288-0 repunit 'ru3' created
Replication>
```

---

**Note:** Destination replication units should be created only at the source cluster using the `Replication> repunit create` command.

---

- 2 To confirm the creation of the replication unit, enter the following:

```
Replication> repunit show verbose
```

```
repunit name: ru3
=====
```

```
fs name:
-----
fs1.fs2
```

```
paths:
-----
fs1/dir1
fs2/dir2
```

```
patterns:
-----
```

```
jobs:
-----
```

You can use the `Replication> repunit add_entry`, `Replication> repunit modify_entry`, `Replication> repunit remove_entry`, and `Replication> repunit destroy` commands to manage your replication units.

---

**Note:** The `Replication> repunit modify_entry`, `Replication> repunit remove_entry`, and `Replication> repunit destroy` operations are not allowed for the replication units that are included in any job definitions.

---

In addition you can use the `Replication> repunit add_pattern_entry` to add entries to the existing replication unit based on a file name pattern matching. File name pattern matching lets you replicate files or directories based on the file name pattern, such as `.log`, `.txt`, `.pdf`, or `.tar`, using globbing.

Repunit pattern entries can be used to define a set of files or directories that are replicated to a target. When at least one repunit pattern entry is defined, files or directories not matching the repunit pattern(s) are not be replicated to the target. The repunit directory pattern entry allows you to only replicate directories without replicating any files. To only replicate directories, you can specify directory pattern(s), without any file pattern. To replicate files with a directory pattern, at least one file pattern (e.g. `/**/*`) should be present in the repunit.

The following file selection priorities apply for path entries and pattern entries:

- Path entries added using the `Replication> exclunit add_entry` command have the highest priority. If any file matches this entry it will be excluded from replication. Also, if any path matches both the repunit and the exclunit, the path is not replicated to the target.
- Path entries added using the `Replication> repunit add_entry` command have the second highest priority.
- Pattern entries added using the `Replication> exclunit` command have the third highest priority. If any path from the replication unit path entry matches the excluding unit pattern, the path is excluded and file is not replicated.
- Pattern entries added using the `Replication> repunit` command have the lowest priority.
- If you configure a replication repunit pattern, only the files matching the pattern are replicated. If you configure an excluding unit pattern, only the files that do not match the pattern are replicated. If both replication repunit and exclunit patterns are configured, the path and the pattern file selection priorities apply.

## To add a pattern entry

- 1 To add a pattern entry to an existing replication unit, enter the following:

```
Replication> repunit add_pattern_entry repunit_name "filesystem/ \
directory_pattern/filename_pattern"
```

*repunit\_name*            The name of the replication unit you want to add the pattern entry to.

*filesystem*            The file system name.

*directory\_pattern*    The pattern you want to apply at the directory level.

*filename\_pattern*    The file name pattern, for example .log, .txt, .pdf, or .tar.

For example:

```
Replication> repunit add_pattern_entry rpul "fs1/**/*.pdf,fs1/**/*.doc"
ACCESS replication SUCCESS V-288-0 repunit pattern add Success.
```

- 2 To confirm the addition of the pattern entry, enter the following:

```
Replication> repunit show verbose
```

```
repunit name: rpul
=====
```

```
fs name:
-----
fs1
```

```
paths:
-----
```

```
patterns:
-----
"fs1/**/*.pdf"
"fs1/**/*.doc"
```

```
jobs:
-----
```

A pattern can be constructed using special characters. The pattern characters are case sensitive. A pattern followed by a slash '/' is considered a directory pattern

and is only matched against directories. A pattern that does not end with a slash '/' is considered as a file pattern and is matched against both files and directories.

[Table 31-1](#) provides a description of special characters that can be specified in the pattern entry.

**Table 31-1** Pattern entry special characters

Character	Description
?	Matches the preceding character one time.
*	Matches the preceding character 0 or more times.
[ ] or [!]	Matches any of the characters that are specified in the square bracket. Specifying [0-5] matches any number from 0 to 5. Using ! inverts the specified characters. For example [!abcd] matches any character other than a, b, c, or d.
Simplified **	Matches any depth of directory after the first directory. For example <code>vx/fs1/*/*.pdf</code> matches any .pdf file in the first depth of the directory after the fs1 first directory, but does not match <code>/vx/fs1/dir1/dep2/a.pdf</code> . To match the second file, use the ** character. For example, <code>/vx/fs1/**/*.pdf</code> . For example <code>vx/fs1/*/*.pdf</code> matches any .pdf file in the first depth of the directory after fs1. In the file list <code>/vx/fs1/a.pdf, /vx/fs1/dir1/b.pdf, /vx/fs1/dir1/dir2/c.pdf</code> , the pattern only matches b.txt. To match files after the current depth, use **. For example, <code>/vx/fs1/**/*.pdf</code> matches files a.pdf, b.pdf and c.pdf, while pattern <code>/vx/fs1/dir1/**/*.pdf</code> matches files b.pdf and c.pdf.
\	Matches any special characters literally in the path.

You can use the `Replication> repunit modify_pattern_entry` and `Replication> repunit remove_pattern_entry` commands to manage pattern entries in your replication units.

You next need to set up the schedule for the replication.

See [“Scheduling the replication”](#) on page 551.

## Setting up files to exclude from a replication unit

Once you have set up the files systems you want to replicate, you can define a set of directories or files to exclude from a replication unit. This step is optional. The `exclunit` entry and the `exclunit` pattern have higher priority over the `repunit` pattern.

If any file name matches the `exclunit` entry or pattern, the file is not replicated to the target.

To work with exclusion units:

- Use the `Replication> exclunit create` command to name the excluding unit and configure the directories and files you want to exclude from a replication. The excluding unit you create can be used in multiple replication jobs. A single excluding unit can span across multiple directories.
- Use the `Replication> job exclude` command to add the excluding unit to a replication job. You cannot add an excluding unit to a job that is active. You must disable the job first.
- You can use the following commands: `Replication> exclunit add_entry`, `Replication> exclunit modify_entry`, and `Replication> exclunit remove_entry` to make changes to an excluding unit, provided the excluding unit you want to modify is not included in any job definitions.
- Use the `Replication> job show` command to show which excluding units are configured for a job. Use the `Replication> exclunit show` command to show the names and contents of all excluding units that are defined for the cluster.
- Use the `Replication> exclunit destroy` command to permanently delete the excluding unit. You can only destroy an excluding unit if the excluding unit you want to destroy is not included in any job definitions.

If a replication is defined for a directory, an excluding unit should be a subset of that directory. The excluding unit cannot be the same directory as the replication and it cannot be a parent directory of the replication. For example, if a replication is configured for `fs1/dir1/dir2`, a valid exclusion could be `dir1/dir2/file` or `dir1/dir2/dir3`, but not `/dir1` (the parent directory for the replication).

By default, Veritas Access excludes some common directories and files from all replication units. These directories and files include:

- `lost+found`
- `.placement_policy.xml`
- `quotas`
- `quotas.grp`
- `quotas.64`
- `quotas.grp.64`

In addition, you can use the `Replication> exclunit` commands to specify additional directories and files to exclude.

The directories and files you specify for an excluding unit are applied based on the overall definition of the replication. For example, a replication job that contains an `fs1` replication unit and an `dir3` excluding unit, replicates all the files in `fs1`, except for the files in `fs1/dir3`.

### To create an excluding unit:

- 1 To create an excluding unit, enter the following:

```
Replication> exclunit create exclunit_name
                exclunit_entry[,exclunit_entry,..]
```

*exclunit\_name* Enter the name of the excluding unit.

*exclunit\_entry* Enter the comma-separated list of directories and files you want to exclude from a replication.

For example:

```
Replication> exclunit create exclul dir1,dir2/file1,dir2/file2
ACCESS replication SUCCESS V-288-1246 exclunit 'exclul' created
```

- 2 To confirm the creation of the excluding unit enter the following:

```
Replication> exclunit show verbose
```

```
exclunit name: exclul
=====
```

```
fs name:
-----
```

```
paths:
-----
dir1,dir2/file1,dir2/file2
```

```
patterns:
-----
```

```
jobs:
-----
```

You can use the `Replication> exclunit add_entry`, `Replication> exclunit modify_entry`, `Replication> exclunit remove_entry`, and `Replication> exclunit destroy` commands to manage your excluding units.

---

**Note:** The `Replication> exclunit add_entry`, `Replication> exclunit modify_entry`, `Replication> exclunit remove_entry`, and `Replication> exclunit destroy` operations are not allowed for excluding units that are included in any job definitions.

---

In addition you can use the `Replication> exclunit add_pattern_entry` to add entries to the existing replication unit based on a file name pattern matching. File name pattern matching lets you specify files or directories to exclude from replication based on the file name pattern, such as `.log`, `.txt`, `.pdf`, or `.tar`, or using a regular expression. A regular expression is a sequence of characters that forms a search pattern, which is primarily used for pattern matching with strings.

### To add a pattern entry

- 1 To add a pattern entry to an existing excluding unit, enter the following:

```
Replication> exclunit add_pattern_entry exclunit_name
"directory_pattern/filename_pattern"
```

*exclunit\_name*            The name of the excluding unit you want to add the pattern entry to.

*directory\_pattern*        The pattern you want to apply at the directory level.

*filename\_pattern*        The file name pattern, for example .log, .txt, .pdf, or .tar.

For example:

```
Replication> exclunit add_pattern_entry ex1 "**/app?*.tmp"
ACCESS replication SUCCESS V-288-0 exclunit pattern add Success.
```

- 2 To confirm the addition of the pattern entry, enter the following:

```
Replication> exclunit show verbose
exclunit name: ex1
=====
```

```
fs name:
-----
```

```
paths:
-----
```

```
dir1/
```

```
patterns:
-----
```

```
"**/app?*.tmp"
```

```
jobs:
-----
```

See [Table 31-1](#) on page 546.

You can use the `Replication> exclunit modify_pattern_entry` and `Replication> exclunit remove_pattern_entry` commands to manage pattern entries in your replication units.

## Scheduling the replication

You use the `Replication> schedule` commands to create a schedule for replicating files from the source to the destination cluster.

Veritas Access Replication supports periodic replications, where the data gets replicated from the source to the destination cluster at regular intervals as defined by the schedule. Veritas Access Replication uses the following parameters to schedule the replication jobs: minute, hour, day-of-the-month, month, and day-of-the-week.

Make sure that you already set up the file systems you want to replicate.

See [“Setting up the file systems to replicate”](#) on page 541.

## To create a replication schedule

- ◆ To create a replication schedule, enter the following:

```
Replication> schedule create schedule_name minute  
[hour] [day_of_the_month] [month] [day_of_the_week]
```

<i>schedule_name</i>	Specify the name of the schedule to be created.
<i>minute</i>	Enter a numeric value between 0-59, or an asterisk (*), which represents every minute. This variable is not optional.
<i>hour</i>	Enter a numeric value between 0-23, or an asterisk (*), which represents every hour.
<i>day_of_the_month</i>	Schedule the day of the month you want to run the replication. Enter a numeric value between 1-31, or an asterisk (*), which represents every day of the month.
<i>month</i>	Schedule the month you want to run the replication. 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 (not case sensitive).
<i>day_of_the_week</i>	Schedule the day of the week you want to run the replication. Enter a numeric value between 0-6, or an asterisk (*), which represents every day of the week. Sunday is interpreted as 0. You can also enter the first three letters of the week (you must use lower case letters).

You can enter an interval (two numbers separated by a hyphen) for the *minute*, *hour*, *day-of-month*, *month*, and *day-of-week*. If you want to run the schedule between 1:00 a.m. and 4:00 a.m., you can enter a value of 1-4 for the hour variable. The range is inclusive

The parameters also accept a set of numbers separated by a comma. For example, 1, 3, 5, 7 or 1-4, 5-10.

For example, to create a schedule where the replication job occurs every 30 minutes, enter:

```
Replication> schedule create s1 */30
```

### To display the list of schedules

- ◆ To display the schedule you have set up for replication, enter the following:

```
Replication> schedule show s1
Schedule Name  Minute   Hour    Day    Month  WeekDay
=====
s1             */30    *       *      *      *
```

You can also use the `Replication> schedule modify` and `Replication> schedule delete` to manage your replication schedules.

---

**Note:** The `Replication> schedule modify` and `Replication> schedule delete` operations are not allowed for the schedules that are included in any job definition.

---

You next need to define what is replicated.

See [“Defining what to replicate”](#) on page 553.

## Defining what to replicate

You use the `Replication> job` commands to set up a job definition. This defined job determines what to replicate and when, using the settings from the previous commands.

Make sure that you created a schedule for replicating files from the source to the destination cluster.

See [“Scheduling the replication”](#) on page 551.

**To set up the replication job**

**1** To create a replication job, enter the following:

```
Replication> job create job_name src_repunit tgt_repunit\  
[,tgt_repunit2,...,tgt_repunitn] link_name\  
[,link_name2,...,link_namen schedule_name [encrypt=yes|no]\  
[metadata_only=yes|no]
```

<i>job_name</i>	Specify a name for the replication job you want to create.
<i>src_repunit</i>	Specify the source replication unit. The replication unit determines the exact item (such as a file system) that you want to replicate.
<i>tgt_repunit</i>	Specify one or more target replication units, separated with a comma.
<i>link_name</i>	Specify one or more link names, separated with a comma, used when you ran the <code>Replication&gt; config auth</code> command between the local cluster and the remote cluster. Both the source cluster and the destination cluster need to be assigned a unique identifier (name). This identifier is used to identify the link that is established between the source and the destination clusters. You can use the link name instead of the virtual IP addresses of the source and the destination clusters when using the other replication commands.
<i>schedule_name</i>	Specify the name of the replication schedule you want to apply to the replication job.

You can specify multiple target replication units and links by separating the target replication units and the link names with commas.

The `encrypt=yes|no` option lets you enable or disable encryption on the replication job. If encryption is enabled, the data is encrypted over the network, providing a secure channel between the source and the target system(s). If this option is not specified, by default the replication job encryption is set to disabled.

When enabling encryption on a replication job you must either generate a self-signed security certificate using the `Replication> config certificate generate` command, or import a trusted security certificate from an external entity using the `Replication> config certificate import` command.

The `metadata_only=yes|no` option lets you replicate the entire file system metadata to a single target node. At each interval a file system point in time image is taken, and only metadata changes are sent to the target.

For example:

```
Replication> job create job1 rul trp1,trp2 new_link1,new_link2 sch1\
encrypt=no metadata_only=yes
```

- 2 To add an excluding unit to the job, enter the following command. This step is optional.

```
Replication> job exclude job_name exclunit_name
```

For example:

```
Replication> job exclude job1 ex1
ACCESS replication SUCCESS V-288-162 Job exclude command completed
successfully.
```

- 3 By default, the job is disabled. To enable the job, enter the following:

```
Replication> job enable job_name
```

For example:

```
Replication> job enable job1
ACCESS replication SUCCESS V-288-1303 Trying to enable job job1.
Please check status of job after a few seconds.
```

- 4 To check if the job was enabled, enter the following:

```
Replication> job show [job_name]
```

For example:

```
Replication> job show job1
Job Name Role Job Type Encryption Debug Schedule State
=====
job1 SOURCE DATA OFF ON sch1 ENABLED

CKPT Count Exclunit Source repunit Target repunit(s) Link name(s)
=====
10 ex1 rul trp1,trp2 new_link1,new_link2
```

## About the maximum number of parallel replication jobs

The maximum number of replication jobs is 64, but there are stricter limits on the number of replication jobs that can be running in parallel at the same time. Replication uses a RAM-based file system for storing the transit messages. Each GB of this RAM-based file system can accommodate up to eight parallel running jobs. The default size of this file system depends upon the amount of physical memory of the node on which replication is running. If the physical memory is less than 5 GB, replication limits its maximum usage for storing messages to 1 GB of memory, which means the user can run up to eight replication jobs in parallel at the same time. If the physical memory is between 5 GB to 10 GB, replication limits its maximum usage for storing messages to 2 GB of memory, which means you can run up to 16 replication jobs in parallel. If the physical memory is greater than 10 GB, replication limits its maximum usage for storing messages to 4 GB of memory, which means you can run up to 32 replication jobs in parallel at the same time.

## Managing a replication job

You can manage a replication job using the `Replication> job` commands. The commands are required only on the source system.

The `Replication> job enable`, `Replication> job sync`, `Replication> job disable`, `Replication> job abort`, `Replication> job pause`, and `Replication> job resume` commands change the status of an existing replication job.

You can use the `Replication> job modify`, `Replication> job add_link`, `Replication> job remove_link`, and `Replication> job destroy` commands to modify or destroy a replication job definition.

The `Replication> job enable` command starts replication immediately and initiates replication after every subsequent set frequency interval. When a replication job is created it is disabled by default, and you must enable the job to start replication.

### To enable a replication job

- ◆ To enable a replication job, type the following command:

```
Replication> job enable job_name
```

*job\_name* Specify the name of the replication job you want to enable.

For example:

```
Replication> job enable job1
ACCESS replication SUCCESS V-288-1303 Trying to enable job job1.
Please check status of job after a few seconds.
```

At each frequency interval, a fresh file system Storage Checkpoint is taken and replication is started against the new Storage Checkpoint. If a previous replication run has not completed, a new Storage Checkpoint is not taken and the current run is skipped.

---

**Note:** Running the `Replication> job enable` command on a previously aborted replication job automatically restarts the job.

---

The `Replication> job sync` command lets you start a replication job, but then stops the replication job after one iteration (full or incremental) is complete. You can use this command to recover from the secondary site in the event that the primary file system is completely destroyed. This command can also be used if you want to run a replication job at a predefined time using a script or a cron job.

See [“Synchronizing a replication job”](#) on page 567.

The `Replication> job disable` command drops the replication job from the schedule and waits for any already running iterations to complete. The `Replication> job disable` command disables a job definition which is in one of these states: ENABLED, PAUSED, or FAILED. This process can take some time if the network is slow or if a large amount of data has changed since the last replication run.

### To disable a replication job

- ◆ To disable a replication job, type the following command:

```
Replication> job disable job_name
```

*job\_name* Specify the name of the replication job you want to stop.

For example:

```
Replication> job disable job1
```

```
ACCESS replication SUCCESS V-288-0 Job 'job1' disabled successfully
```

The `Replication> job abort` command forcefully cancels a replication job even if it is in progress. Aborting a replication job may leave Storage Checkpoints mounted on the source system and the target file system may be left in an intermediate state.

### To abort a replication job

- ◆ To abort a replication job, type the following command:

```
Replication> job abort job_name
```

*job\_name* Specify the name of the replication job you want to abort.

For example:

```
Replication: job abort job1
```

The `Replication> job pause` command immediately stops the replication job. You must use the `Replication> job resume` command to resume the replication job from where it was paused. When replication is resumed, the replication job replicates the set of selected files before pausing the job, and attempts to replicate as much of the latest data as possible. This action allows the customer to have two recovery point objectives (RPO). When the replication job is paused, the replication frequency option is disabled. Once the replication job is resumed, the frequency option resumes for subsequent iterations. The pause and the resume functions let you manage the replication job based on workload requirements.

**To pause and resume a replication job**

- 1 To pause a replication job, type the following command:

```
Replication> job pause job_name
```

where *job\_name* is the name of the replication job you want to pause.

- 2 To resume a replication job, type the following command:

```
Replication> job resume job_name
```

where *job\_name* is the name of the replication job you want to resume.

---

**Note:** You cannot start or sync a paused job. You can abort a paused job. However, if synchronization is performed on a paused job that has been aborted, the last RPO for the paused job is not available.

---

The `Replication> job modify` command lets you modify debugging, encryption and the number of replication Storage Checkpoints on a replication job definition.

The addition or removal of a filesystem from the source replication unit or the destination replication unit is not supported. To remove a specific filesystem from the replication unit you must destroy the replication job and recreate the replication job with the new set of file systems in the replication unit. To add a specific filesystem from an existing replication unit, you can either create a new replication job with a new source replication unit and target replication unit, or destroy the replication job and recreate it with the new set of file systems in the replication unit to use the same job name

The `Replication> job modify debug` command lets you enable or disable debugging on a given job.

**To modify debugging on a replication job**

- ◆ To modify debugging on a replication job definition, enter the following command:

```
Replication> job modify debug job_name on|off
```

*job\_name*                      Specify the replication job name you want to modify.

The `Replication> job modify encrypt` command lets you enable or disable encryption on a given job.

### To modify encryption on a replication job

- ◆ To modify encryption on a replication job definition, enter the following command:

```
Replication> job modify encrypt job_name on|off
```

*job\_name* Specify the replication job name you want to modify.

When enabling encryption on a replication job you must either generate a self-signed security certificate using the `Replication> config certificate generate` command, or import a trusted security certificate from an external entity using the `Replication> config certificate import` command.

The `Replication> job modify rep_dest_ckpt_cnt` command lets you set the number of replication Storage Checkpoints you want to keep at the destination cluster. The default value is 10, and the valid range is 1 to 10.

### To modify the number of replication Storage Checkpoints on a replication job

- ◆ To modify the number of replication Storage Checkpoints on a replication job definition, enter the following command:

```
Replication> job modify rep_dest_ckpt_cnt job_name ckpt_cnt
```

*job\_name* Specify the replication job name you want to modify.

*ckpt\_cnt* Specify the Storage Checkpoint count (1-10).

The `Replication> job add_link` and `Replication> job remove_link` commands let you add or remove a link from an existing replication job. The link name is used to identify the link that is established between the source and the destination clusters. You can use the link name instead of the virtual IP addresses of the source and destination clusters when using replication commands. The link name is established when running the `Replication> config auth` command between the local cluster and the remote cluster.

See [“Setting up communication between the source and the destination clusters”](#) on page 528.

In addition, the `Replication> job add_link` command lets you enable or disable non-empty target replication using the `delete_extra_files` option. For example, if there are conflicting files or paths on both the source and the target system, the replication job fails. You can enable the `delete_extra_files` option to check for and delete any conflicting files or directories before replication. By default, this option is set to `no`.

### To add a link to an existing replication job

- ◆ To add a link to an existing replication job, enter the following command:

```
Replication> job add_link job_name tgt_repunit\  
link_name [delete_extra_files=yes|no]
```

*job\_name* Specify the replication job name you want to add a link to.

*tgt\_repunit* Specify the target replication unit(s).

*link\_name* Specify the link name(s) you want to add to the replication job.

For example:

```
Replication> job add_link job1 trp1 new_link1 delete_extra_files=yes
```

You can specify multiple target replication units and links by separating the target replication units and the link names with commas.

### To remove a link from an existing replication job

- ◆ To remove a link from an existing replication job, enter the following command:

```
Replication> job remove_link job_name link_name [force=yes|no]
```

*job\_name* Specify the replication job name you want to remove a link from.

*link\_name* Specify the link name you want to remove from the replication job.

*force* Specify the *force=yes* option to stop replication if the target is actively replicating. The target is also marked for removal.

For example:

```
Replication> job remove_link job1 new_link1
```

You can specify one or more links to remove from a replication job by separating the link names with commas.

If the target is actively replicating, then use the *force* option to stop replication for the target and mark it for removal.

For example:

```
Replication> job remove_link job1 new_link1 force=yes
```

To enable non-empty target replication on an existing replication job, you must remove, and then re-add the link with the *delete\_extra\_files* option enabled.

**To enable non-empty target replication on an existing replication job**

- 1 Remove the link from the existing replication job:

```
Replication> job remove_link job_name link_name
```

For example:

```
Replication> job remove_link job1 link1
```

- 2 Add the link back with the `delete_extra_files=yes` option:

```
Replication> job add_link job_name tgt_repunit\  
link_name delete_extra_files=yes
```

For example:

```
Replication> replication job add_link job1 tgt_rpl link1\  
delete_extra_files=yes
```

- 3 Sync the replication job:

```
Replication> job sync job_name
```

For example:

```
Replication> job sync job1
```

The `Replication> job destroy` command destroys a job definition. This command completely removes the specified job from the configuration, cleans up any saved job-related statistics, and removes any Storage Checkpoints. The replication job must be disabled before the job definition can be destroyed.

### To destroy a replication job definition

- ◆ To destroy a job definition, enter the following command:

```
Replication> job destroy job_name
```

Where *job\_name* is the name of the job definition you want to delete. Make sure that the job is not enabled.

Using the `Replication> job destroy` command with the `force` option removes the local job irrespective of the job state, and all replication units are disassociated from the job. Cluster configurations, which are part of the job, are not modified.

For example:

```
Replication> job destroy job1
```

---

**Note:** When setting up replication, Veritas does not advise you to make any modifications or deletions on the target side of the file system. In the event that some or all of the target data is modified or deleted, you must re-create the replication job from the source cluster to resume replication services

---

### To re-create a replication job

- 1 To re-create a replication job, you must first delete the job definition. Enter the following command on the source cluster:

```
Replication> job destroy job_name
```

Where *job\_name* is the name of the job definition you want to delete. Make sure that the job is not enabled.

For example:

```
Replication> job destroy job1
```

- 2 Re-create the job definition:

```
Replication> job create job_name src_repunit tgt_repunit \  
link_name schedule_name
```

For example:

```
Replication> job create job1 rul1 trp1 new_link1 sch1
```

You can reuse the source replication unit, target replication unit, link, and schedule names.

- 3 If there is data available on the target cluster, remove the target link:

```
Replication> job remove_link job_name link_name
```

For example:

```
Replication> job remove_link job1 new_link1
```

- 4 Add the target link with the `delete_extra_files` option enabled:

```
Replication> job add_link job_name tgt_repunit\  
link_name delete_extra_files=yes
```

For example:

```
Replication> job add_link job1 trp1 new_link1 delete_extra_files=yes
```

## Replicating compressed data

Using the `vxcompress` utility, Replication is able to replicate any compressed file that is created at the source to the target, while maintaining the same compression characteristics. The compression characteristics include the algorithm, the strength, and the block size. The data is read in the compressed format from the source, sent over the network, and written to the target system in the same format. This form of compression reduces the amount of storage that is required on the target system.

---

**Note:** Compressed files that are created using archive utilities such as `.tar` or `.zip`, are treated as normal data files and not compressed during replication.

---

## Displaying replication job information and status

The `Replication> job show` and `Replication> job status` commands display job definition information, which allows you to confirm any changes that are made to your replication job and view current job status.

The `Replication> job show` command displays single job definition, or all of the job definitions for a destination cluster.

**To display the job definitions**

- ◆ To display the job definitions, enter the following command:

```
Replication> job show [job_name]
```

*job\_name*            Enter the name of the job you want to display. If you want to list all of the job definitions, enter the command without a job name.

For example, to display a job definition:

```
Replication> job show job1
```

```
Job Name Role   Job Type Encyrption Debug Schedule State
===== =====
job1      SOURCE DATA   OFF      ON    sch1    ENABLED

CKPT Count Exclunit Source repunit Target repunit(s) Link name(s)
===== =====
10         ex1      ru1          trp1, trp2          new_link1, new_link2
```

The `Replication> job status` command displays the status of one or all of the jobs that are copied during replication and the time the replication occurred.



## Behavior of the file systems on the replication destination target

Destination file systems are mounted as read-write. Read-only access is allowed, but you are not expected to modify the destination file system content. While replication occurs, destination file systems may not be in a consistent state. To provide consistent images of the destination file systems at different stages of the replication, the replication service creates and manages Storage Checkpoints of each destination file system.

The replication service creates a new destination Storage Checkpoint:

- Before the first session (before a full-sync)
- After every successful replication session (after every incremental sync)

Storage Checkpoints are automatically mounted under the `.checkpoint` directory inside the target file system, for example:

```
/vx/target_mount/.checkpoint/ckpt_name
```

where *target\_mount* is the name of the target file system and *ckpt\_name* is the name of the Storage Checkpoint.

You can use the `Storage> snapshot list` command to view these Storage Checkpoints and you can use Veritas Access commands to export any of these Storage Checkpoints for read-only purposes. The replication Storage Checkpoint names are prefixed with `vxfssrepl_` and also contain the Storage Checkpoint creation time.

Storage Checkpoint storage is configurable. You can use the `Replication> job modify rep_dest_ckpt_cnt job_name ckpt_cnt` command to specify how many destination Storage Checkpoints you want to keep for each job. The default value is 10.

## Accessing file systems configured as replication destinations

Destination Storage Checkpoints are automatically mounted and therefore cannot be brought online or taken offline using the `Storage> snapshot` commands. The destination Storage Checkpoints can only be accessed through the `.checkpoint` directory. This accessibility also applies to any user created Storage Checkpoints on the replication destination file system.

# Creating a recovery point objective (RPO) report

A recovery point is the last stable version of a set of data that can be used to recover from a site failure. A recovery point objective (RPO) is a goal set by an organization to define how much data an organization is willing to lose in the event of an outage. RPO is measured in terms of minutes (or hours) of data lost. For example, a company might have an RPO goal of two hours, which means no more than two hours of data should be lost because of a site failure.

Veritas Access replication tracks the times that are associated with replication jobs and enables you to generate an RPO report to help you manage your organization's RPO objectives. The RPO report shows the current RPO times for a replication job. The report also shows the average RPO times over the last 24 hours, the last week, and the last month.

## To create an RPO report

- ◆ To create an RPO report, enter the following:

```
Replication> rpo show job_name [duration]
```

*job\_name*            Enter the name of the replication job that is associated with the RPO report.

*duration*            To show the average RPO over a specific number of hours, enter a numeric value to indicate the duration in hours. For example, enter 5 to show the average RPO values over the last five hours. The range of hours you can specify is 1 to 712.

For example, to show an RPO report for a job:

```
Replication> rpo show job1
```

```
Replication> rpo show
```

```
JOB    CURRENT RPO LAST 24 AVG RPO LAST 1 WEEK AVE RPO LAST 1 MONTH AVE RPO
=====
Job1   20:17 Secs   1:05:20 Seconds 30:10 Seconds                    45:40 Seconds
```

To show the average RPO for job 1 over the last five hours:

```
Replication> rpo show job1 5
```

```
ACCESS replication INFO V-288-1590
Avg RPO from last 5 hr: 30:35 Seconds
```

# Replication job failover and failback

Typically, the source cluster drives a replication session. However, in some situations, it may be useful for the destination cluster to drive the replication session. Veritas Access supports a failover and a failback feature for replication jobs. This feature enables control of replication jobs to be temporarily relocated from the source cluster to the destination (target) cluster.

Job failover and failback is useful for:

- **Planned failover**  
In cases where the source cluster is taken down for routine maintenance or for moving applications to another cluster, a planned failover procedure is available for moving replication jobs from the source cluster to the destination cluster.
- **Disaster recovery**  
In cases where the source cluster fails unexpectedly, an unplanned failover procedure is available for moving replication jobs to the destination cluster.

---

**Note:** In the event of a planned or unplanned failover from the source cluster to the destination cluster, there should be at least one successful sync attempt. The successful sync ensures that a consistent point in time image is present on the destination cluster that can be used for the failover.

---

With job failover and failback, you use the `Replication> job failover` command to move control from the source cluster to the destination cluster. You use the `Replication> job failback` to restore control to the source cluster. The `link_name` is the link of one of the destination clusters. The `link_name` argument can be empty when the source cluster is not available, in which case the job failover can be executed from one of the destination clusters.

Essentially, job failover takes job and replication unit definitions from the replication database on the source cluster and copies them to the replication database on the destination cluster.

---

**Warning:** Job failover assumes that all replication job names and replication unit names are unique across all Veritas Access clusters on your network. Before you use the replication failover feature, make sure that these names are unique.

---

After a job failover or failback, you must manually start or enable the replication job to start pre-configured schedules. Link throttle information should be reconfigured after the job failover or failback.

Job failover does not automatically move the NFS or the CIFS share information that is associated with job failover replication units from the source cluster to the destination cluster. Share information has to be done manually.

**Table 31-2** Job failover and failback commands

Command	Definition
<code>job failover</code>	Transfer control of a replication job from the source cluster to the destination cluster.
<code>job failback</code>	Return control of a replication job from the destination cluster to the source cluster.

## Process summary

The steps you take for job failover and failback vary depending the type of failover or failback you perform. Failover and failback types include:

- Planned failover
- Unplanned failover
- Failback after a planned failover
- Failback after an unplanned failover

Each process is summarized in the following sections. Typically, you would use the planned failover and planned failback processes in most situations.

## Overview of the planned failover process

This section shows an overview of the steps you take to perform a planned failover.

For planned failovers, most of the failover steps are executed from the source cluster.

- From the source cluster:
  - Stop all applications that access the replicated files. This step is recommended, but not required.
  - Use the `Replication> job sync job_name` command to execute the job and make sure files on the source cluster and destination cluster are synchronized.
  - Use the `Replication> job disable job_name` command to disable the job.

- Use the `Replication> job failover job_name link_name` command to move control of the job from the source cluster to the destination cluster.
- From the destination cluster:
  - Use the `Replication> job enable job_name` command to enable the job on the destination cluster.
  - Use the `Replication> bwlimit reset link_names` command to reset link throttle information on the new source cluster.
  - Use the `Replication> job sync job_name` command to ensure that the replication job is in a well-defined state and incremental replication can be resumed.

Once the job is failed over, job control remains on the destination cluster until a planned failback is activated.

See [“Overview of the planned failback process”](#) on page 572.

## Overview of the planned failback process

After a job failover has been accomplished and the source cluster is ready to take back control of the replication task, you can use the job failback feature to release control from the destination cluster and return it to the source cluster

- From the destination cluster:
  - Stop all applications that access the replicated files. This step is recommended, but not required.
  - Use the `Replication> job sync job_name` command to execute the job and make sure files on the source cluster and destination cluster are synchronized.
  - Use the `Replication> job disable job_name` command to disable the job.
- From the source cluster:
  - Use the `Replication> job failback job_name` command to move control of the job from the destination cluster back to the original source cluster.
  - Use the `Replication> job enable job_name` command to enable the job on the source cluster.
  - Use the `Replication> job sync job_name` command to ensure that the replication job is in a well-defined state and incremental replication can be resumed.

## Overview of the unplanned failover process

In some cases (for example, unexpected equipment failure), you may need to execute an unplanned failover for replication jobs. The unplanned failover process differs from the planned failover process.

This section shows an overview of the steps you take to perform an unplanned failover.

For unplanned failovers, all the commands are executed from the destination cluster.

- Make sure that you are logged into the destination cluster.
- Use the `Replication> job disable job_name` command to disable the job from the destination cluster. When you execute the `Replication> job disable` command from the destination cluster.
- Use the `Replication> job failover job_name` command to failover the job.

## Overview of the unplanned failback process

After an unplanned failover, when the source cluster comes up, you can use the following unplanned failback process to return control to the original source cluster:

- Make sure that you are logged into the source cluster.
- Use the `Replication> job failback job_name link_to_new_source` command to configure the current source cluster as a valid target to the new source cluster. This command should be executed from the old source cluster.
- Use the `Replication> job sync job_name` command from the new source cluster to synchronize file system data with the newly added destination cluster.
- Use the `Replication> job failover job_name link_to_old_source` command to move control of the replication job from the destination cluster back to the source cluster.
- Use the `Replication> job sync job_name` command to ensure that the replication job is in a well-defined state and incremental replication can be resumed.

---

**Note:** An administrator can use the `Replication> job destroy force` command to clean up local job configuration. Configuration of the other clusters, which are part of the job, will not be modified and any replication units will be disassociated from job. The `Replication> job destroy force` and `Replication> repunit destroy force` commands should be used in the event of an unrecoverable configuration or replication direction mismatch.

---

# Using snapshots

This chapter includes the following topics:

- [About snapshots](#)
- [Creating snapshots](#)
- [Displaying snapshots](#)
- [Managing disk space used by snapshots](#)
- [Bringing snapshots online or taking snapshots offline](#)
- [Restoring a snapshot](#)
- [About snapshot schedules](#)
- [Configuring snapshot schedules](#)
- [Managing automated snapshots](#)

## About snapshots

A snapshot is a virtual image of the entire file system. You can create snapshots of a parent file system on demand. Physically, it contains only data that corresponds to the changes that are made in the parent, and so consumes significantly less space than a detachable full mirror.

---

**Note:** You cannot create a snapshot of a scale-out file system.

---

See [“About scale-out file systems”](#) on page 335.

Snapshots are used to recover from data corruption. If files, or an entire file system, are deleted or become corrupted, you can replace them from the latest uncorrupted snapshot. You can mount a snapshot and export it as if it were a complete file

system. Users can then recover their own deleted or corrupted files. You can limit the space snapshots consume by setting a quota on them. If the total space that snapshots consume exceeds the quota, Veritas Access rejects attempts to create additional ones.

You can create a snapshot by either using the `snapshot create` command or by creating a schedule to create the snapshot at a specified time.

## Creating snapshots

The `snapshot create` command quickly creates a persistent image of a file system at an exact point in time. Snapshots minimize the use of disk space by using a Storage Checkpoint within the same free space available to the file system. After you create a snapshot of a mounted file system, you can also continue to create, remove, and update files on the file system without affecting the logical image of the snapshot. A snapshot preserves not only the name space (directory hierarchy) of the file system, but also the user data as it existed at the moment the file system image was captured.

You can use a snapshot in many ways. For example, you can use them to:

- Create a stable image of the file system that can be backed up to tape.
- Provide a mounted, on-disk backup of the file system so that end users can restore their own files in the event of accidental deletion. This is especially useful in a home directory, engineering, or email environment.
- Create an on-disk backup of the file system that can be used in addition to a traditional tape-based backup to provide faster backup and restore capabilities.

### To create a snapshot

- ◆ To create a snapshot, enter the following:

```
Storage> snapshot create snapshot_name  
          fs_name [removable]
```

`snapshot_name`            Specifies the name for the snapshot.

**Note:** The following are reserved words for snapshot name:  
`flags`, `ctime`, and `mtime`.

`fs_name`                 Specifies the name for the file system.

removable

Valid values are:

- yes
- no

If the removable attribute is `yes`, the snapshot is removed automatically if the file system runs out of space.

The default value is `removable=no`.

For example:

```
Storage> snapshot create snapshot1 fs1
100% [#] Create snapshot
```

## Displaying snapshots

You can display all snapshots, or the snapshots taken of a specific file system or specific schedule of a file system. The output displays the snapshot name and the properties of the snapshots such as creation time and size.

**To display snapshots**

- ◆ To display snapshots, enter the following:

```
Storage> snapshot list [fs_name] [schedule_name]
```

**fs\_name** Displays all of the snapshots of the specified file system. If you do not specify a file system, snapshots of all of the file systems are displayed.

**schedule\_name** Displays the schedule name. If you do not specify a schedule name, then snapshots created under *fs\_name* are displayed.

```
Storage> snapshot list
Snapshot
=====
snap2                fs1  offline
sc1_24_Jul_2009_21_34_01_IST  fs1  offline
sc1_24_Jul_2009_19_34_02_IST  fs1  offline
presnap_sc1_24_Jul_2009_18_34_02_IST  fs1  offline
sc1_24_Jul_2009_17_34_02_IST  fs1  offline

ctime                mtime                Removable Preserved Size
=====
2009.Jul.27.02:40:43 2009.Jul.27.02:40:57 no          No          190.0M
2009.Jul.24.21:34:03 2009.Jul.24.21:34:03 yes         No          900.0M
2009.Jul.24.19:34:04 2009.Jul.24.19:34:04 yes         No          7.0G
2009.Jul.24.18:34:04 2009.Jul.24.18:34:04 yes         Yes         125M
2009.Jul.24.17:34:04 2009.Jul.24.17:34:04 yes         No          0K
```

**Snapshot** Displays the name of the created snapshots.

**FS** Displays the file systems that correspond to each created snapshots.

**Status** Displays whether or not the snapshot is mounted (that is, online or offline).

**ctime** Displays the time the snapshot was created.

**mtime** Displays the time the snapshot was modified.

**Removable** Determines if the snapshot should be automatically removed in case the underlying file system runs out of space. You entered either yes or no in the `snapshot create snapshot_name fs_name [removable]`

**Preserved** Determines if the snapshot is preserved when all of the automated snapshots are destroyed.

**Size** Displays the size of the snapshot.

## Managing disk space used by snapshots

To manage the disk space used by snapshots, you can set a snapshot quota or capacity limit for the file system. When all of the snapshots for the file system exceed the capacity limit, snapshot creation is disabled for the file system.

You can also remove unnecessary snapshots to conserve disk space.

## To enable snapshot quotas

- 1 To display snapshot quotas, enter the following:

```
Storage> snapshot quota list
FS           Quota       Capacity Limit
==          =====
fs1          on           1G
fs2          off          0
fs3          off          0
```

- 2 To enable a snapshot quota, enter the following:

```
Storage> snapshot quota on fs_name [capacity_limit]
```

<code>fs_name</code>	Specifies the name of the file system.
<code>capacity_limit</code>	Specifies the number of blocks used by all the snapshots for the file system. Enter a number followed by K, M, G, or T (for kilo, mega, giga, or terabyte). The default value is 0.

For example, to enable the snapshot quota, enter the following:

```
Storage> snapshot quota on fs1 1024K
Storage> snapshot quota list
FS           Quota       Capacity Limit
==          =====
fs1          ON           1024K
```

- 3 If necessary, you can disable snapshot quotas. You can retain the value of the capacity limit. To disable a snapshot quota, enter the following:

```
Storage> snapshot quota off [fs_name] [remove_limit]
```

<code>fs_name</code>	Specifies the name of the file system.
<code>remove_limit</code>	Specifies whether to remove the capacity limit when you disable the quota. The default value is true, which means that the quota capacity limit is removed. The value of false indicates that the quota is disabled but the value of the capacity limit remains unchanged for the file system.

For example, to disable the snapshot quota, enter the following:

```
Storage> snapshot quota off fs1
```

### To destroy a snapshot

- ◆ To destroy a snapshot, enter the following:

```
Storage> snapshot destroy snapshot_name
                        fs_name
```

**snapshot\_name** Specifies the name of the snapshot to be destroyed.

**fs\_name** Specifies the name of the file system from which the snapshot was taken. Snapshots with the same name could exist for more than one file system. In this case, you must specify the file system name.

For example:

```
Storage> snapshot destroy snapshot1 fs1
100% [#] Destroy snapshot
```

## Bringing snapshots online or taking snapshots offline

If you want to mount a snapshot through NFS or export a CIFS snapshot, you must bring the snapshot online. You can then create a CIFS or an NFS share using the snapshot name as the path. For example: `/vx/fs1:snap1`. The snapshot can only be mounted through NFS or exported through CIFS if it is online.

### To bring a snapshot online

- ◆ To bring a snapshot online:

```
Storage> snapshot online snapshot_name fs_name
```

**snapshot\_name** Specifies the name of the snapshot.

**fs\_name** Specifies the name of the file system from which the snapshot was taken. Snapshots with the same name could exist for more than one file system. In this case, you must specify the file system name.

For example, to bring a snapshot online, enter the following:

```
Storage> snapshot online snapshot1 fs1
100% [#] Online snapshot
```

### To take a snapshot offline

- ◆ To take a snapshot offline:

```
Storage> snapshot offline snapshot_name fs_name
```

**snapshot\_name** Specifies the name of the snapshot.

**fs\_name** Specifies the name of the file system from which the snapshot was taken. Snapshots with the same name could exist for more than one file system. In this case, you must specify the file system name.

For example, to take a snapshot offline, enter the following:

```
Storage> snapshot offline snapshot1 fs1  
100% [#] Offline snapshot
```

## Restoring a snapshot

This operation restores the file system to the state that is stored in the specified snapshot. When you restore the file system to a particular snapshot, snapshots taken after that point in time are no longer relevant. The restore operation also deletes these snapshots.

The restore snapshot operation prompts you for confirmation. Be sure that you want to restore the snapshot before responding yes.

### To restore a snapshot

- ◆ To restore a snapshot, enter the following:

```
Storage> snapshot restore snapshot_name
                        fs_name
```

*snapshot\_name* Specifies the name of the snapshot to be restored.

*fs\_name* Specifies the name of the file system to be restored.

For example:

```
Storage> snapshot restore snapshot0 fs0
ACCESS snapshot WARNING V-288-0 Snapshot created after snapshot0
will be deleted
ACCESS snapshot WARNING V-288-0 Are you sure you want to restore
file system fs0 with snapshot snapshot0? (yes/no)
yes
ACCESS snapshot SUCCESS V-288-0 File System fs0 restored
successfully by snapshot snapshot0.
```

## About snapshot schedules

The `Storage> snapshot schedule` commands let you automatically create or remove snapshots for a file system at a specified time. The schedule indicates the time for the snapshot operation as values for minutes, hour, day-of-the-month, month, and day-of-the-week. The schedule stores these values in the crontab along with the name of the file system.

For example, `snapshot schedule create schedule1 fs1 30 2 * * *` automatically creates a snapshot every day at 2:30 AM, and does not create snapshots every two and a half hours. If you wanted to create a snapshot every two and a half hours with at most 50 snapshots per schedule name, then run `snapshot schedule create schedule1 fs1 50 */30 */2 * * *`, where the value `*/2` implies that the schedule runs every two hours. You can also specify a step value for the other parameters, such as day-of-month or month and day-of-week as well, and you can use a range along with a step value. Specifying a range in addition to the `numeric_value` implies the number of times the crontab skips for a given parameter.

Automated snapshots are named with the schedule name and a time stamp corresponding to their time of creation. For example, if a snapshot is created using

the name `schedule1` on February 27, 2016 at 11:00 AM, the name is:  
`schedule1_Feb_27_2016_11_00_01_IST`.

---

**Note:** If the master node is being rebooted, snapshot schedules will be missed if scheduled during the reboot of the master node.

---

## Configuring snapshot schedules

You can use snapshot schedules to automate creation of snapshots at regular intervals. The snapshot limit defines how many snapshots to keep for each schedule.

In some instances, snapshots may skip scheduled runs.

This may happen because of the following:

- When a scheduled snapshot is set to trigger, the snapshot needs to gain a lock to begin the operation. If any command is issued from the CLI or is running through schedules, and if the command holds a lock, the triggered snapshot schedule is not able to obtain the lock, and the scheduled snapshot fails.
- When a scheduled snapshot is set to trigger, the snapshot checks if there is any instance of a snapshot creation process running. If there is a snapshot creation process running, the scheduled snapshot aborts, and a snapshot is not created.

### To create a snapshot schedule

- ◆ To create a snapshot schedule, enter the following:

```
Storage> snapshot schedule create schedule_name
      fs_name
      max_snapshot_limit
      minute [hour] [day_of_the_month]
      [month] [day_of_the_week]
```

For example, to create a schedule for an automated snapshot creation of a given file system at 3:00 am every day, enter the following:

```
Storage> snapshot schedule create schedule1 fs1 100 0 3 * * *
```

When an automated snapshot is created, the entire date value is appended, including the time zone.

<code>schedule_name</code>	<p>Specifies the name of the schedule corresponding to the automatically created snapshot.</p> <p>The <code>schedule_name</code> cannot contain an underscore ('_') as part of its value. For example, <code>sch_1</code> is not allowed.</p>
<code>fs_name</code>	<p>Specifies the name of the file system. The file system name should be a string.</p>
<code>max_snapshot_limit</code>	<p>Specifies the number of snapshots that can be created for a given file system and schedule name. The value is a numeric value between 1-366.</p> <p>When the number of snapshots reaches the limit, then the oldest snapshot is destroyed. If you decrease the limit for an existing schedule, then multiple snapshots may be destroyed (oldest first) until the number of snapshots is less than the maximum snapshot limit value.</p> <p><b>Note:</b> If you need to save daily snapshots for up to one year, the <code>max_snapshot_limit</code> is 366.</p>
<code>minute</code>	<p>This parameter may contain either an asterisk like <code>*/15</code>, which implies every 15 minutes, or a numeric value between 0-59.</p> <p><b>Note:</b> If you are using the <code>*/xx</code> format, the smallest value for 'xx' is 15.</p> <p>You can enter <code>*/(15-59)</code> or a range such as <code>23-43</code>. An asterisk (*) is not allowed.</p>
<code>hour</code>	<p>This parameter may contain either an asterisk, (*), which implies "run every hour," or a number value between 0-23.</p> <p>You can enter <code>*/(0-23)</code>, a range such as <code>12-21</code>, or just the <code>*</code>.</p>
<code>day_of_the_month</code>	<p>This parameter may contain either an asterisk, (*), which implies "run every day of the month," or a number value between 1-31.</p> <p>You can enter <code>*/(1-31)</code>, a range such as <code>3-22</code>, or just the <code>*</code>.</p>
<code>month</code>	<p>This parameter may contain either an asterisk, (*), which implies "run every month," or a number value between 1-12.</p> <p>You can enter <code>*/(1-12)</code>, a range such as <code>1-5</code>, or just the <code>*</code>. You can also enter the first three letters of any month (must use lowercase letters).</p>
<code>day_of_the_week</code>	<p>This parameter may contain either an asterisk (*), which implies "run every day of the week," or a numeric value between 0-6. Crontab interprets 0 as Sunday. You can also enter the first three letters of the week (must use lowercase letters).</p>

For example, the following command creates a schedule `schedule1` for automated snapshot creation of the `fs1` file system every 3 hours each day, and maintains only 30 snapshots:

```
Storage> snapshot schedule create schedule1 fs1 30 0 */3 * * *
```

### To modify a snapshot schedule

- ◆ To modify a snapshot schedule, enter the following:

```
Storage> snapshot schedule modify schedule_name
      fs_name
      max_snapshot_limit
      minute [hour]
      [day_of_the_month] [month] [day_of_the_week]
```

For example, to modify the existing schedule so that a snapshot is created at 2:00 am on the first day of the week, enter the following:

```
Storage> snapshot schedule modify schedule1 fs1 *2**1
```

### To display a snapshot schedule

- ◆ To display all of the schedules for automated snapshots, enter the following:

```
Storage> snapshot schedule show [fs_name] [schedule_name]
```

<b>fs_name</b>	Displays all of the schedules of the specified file system. If no file system is specified, schedules of all of the file systems are displayed.
<b>schedule_name</b>	Displays the schedule name. If no schedule name is specified, then all of the schedules created under <i>fs_name</i> are displayed.

For example, to display all of the schedules for creating or removing snapshots to an existing file system, enter the following:

```
Storage> snapshot schedule show fs3
```

FS	Schedule Name	Max Snapshot	Minute	Hour	Day	Month	WeekDay
===	=====	=====	=====	=====	=====	=====	=====
fs3	sched1	30	*/20	*	*	*	*
fs3	sched2	20	*/45	*	*	*	*

For example, to list the automated snapshot schedules for all file systems, enter the following:

```
Storage> snapshot schedule show
```

FS	Schedule Name	Max Snapshot	Minute	Hour	Day	Month	WeekDay
===	=====	=====	=====	=====	=====	=====	=====
fs6	sc1	10	*/50	*	*	*	*
fs1	sc1	10	*/25	*	*	*	*

# Managing automated snapshots

You can remove all of the automated snapshots created by a schedule, specify that certain snapshots be preserved, or delete a schedule for a file system.

## To remove all snapshots

- ◆ To automatically remove all of the snapshots created under a given schedule and file system name (excluding the preserved and online snapshots), enter the following:

```
Storage> snapshot schedule destroyall schedule_name
fs_name
```

The `destroyall` command only destroys snapshots that are offline. If some of the snapshots in the schedule are online, the command exists at the first online snapshot.

---

**Note:** The `Storage> snapshot schedule destroyall` command may take a long time to complete depending on how many snapshots are present that were created using schedules.

---

Preserved snapshots are never destroyed automatically or as part of the `destroyall` command.

**Example 1:** If you try to destroy all automated snapshots when two of the automated snapshots are still mounted, Veritas Access returns an error. No snapshots under the given schedule and file system are destroyed.

```
Storage> snapshot schedule destroyall schedule1 fs1
ACCESS snapshot ERROR V-288-1074 Cannot destroy snapshot(s)
schedule1_7_Dec_2009_17_58_02_UTC schedule1_7_Dec_2009_16_58_02_UTC
in online state.
```

**Example 2:** If you try to destroy all automated snapshots (which are in an offline state), the operation completes successfully.

```
Storage> snapshot schedule destroyall schedule2 fs1
100% [#] Destroy automated snapshots
```

**To preserve snapshots**

- ◆ To preserve the specified snapshots corresponding to an existing schedule and specific file system name, enter the following:

```
Storage> snapshot schedule preserve schedule_name
           fs_name snapshot_name
```

*snapshot\_name* is a comma-separated list of snapshots..

For example, to preserve a snapshot created according to schedule1 for the file system fs1, enter the following:

```
Storage> snapshot schedule preserve schedule1 fs1
schedule1_Feb_27_16_42_IST
```

**To delete a snapshot schedule**

- ◆ To delete a snapshot schedule, enter the following:

```
Storage> snapshot schedule delete fs_name [schedule_name]
```

For example:

```
Storage> snapshot schedule delete fs1
```

# Using instant rollbacks

This chapter includes the following topics:

- [About instant rollbacks](#)
- [Creating a space-optimized rollback](#)
- [Creating a full-sized rollback](#)
- [Listing Veritas Access instant rollbacks](#)
- [Restoring a file system from an instant rollback](#)
- [Refreshing an instant rollback from a file system](#)
- [Bringing an instant rollback online](#)
- [Taking an instant rollback offline](#)
- [Destroying an instant rollback](#)
- [Creating a shared cache object for Veritas Access instant rollbacks](#)
- [Listing cache objects](#)
- [Destroying a cache object of a Veritas Access instant rollback](#)

## About instant rollbacks

Instant rollbacks are volume-level snapshots. All rollback commands take a file system name as an argument and perform operations on the underlying volume of that file system.

---

**Note:** If you plan to add a tier to the file system, add the tier first and then create the rollback. If you add the tier after a rollback exists, the rollback hierarchy would have inconsistencies because the rollback is not aware of the tier.

---

Both space-optimized and full-sized rollbacks are supported by Veritas Access. 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-write mechanism may degrade the performance of the volume. Full-sized rollbacks use more storage, but that has little impact on write performance after synchronization is completed.

Both space-optimized rollbacks and full-sized rollbacks can be used instantly after operations such as create, restore, or refresh.

---

**Note:** When instant rollbacks exist for a volume, you cannot disable the FastResync option for a file system.

---

When creating instant rollbacks for volumes bigger than 1T, there may be error messages such as the following:

```
ACCESS instant_snapshot ERROR V-288-1487 Volume prepare for full-fs1-1 failed.
```

An error message may occur because the default amount of memory allocated for a Data Change Object (DCO) may not be large enough for such big volumes. You can use the `vxtune` command to change the value. The default value is 6M, which is the memory required for a 1T volume.

To change it to 15M, use the following command:

```
vxtune volpagemod_max_memsz `expr 15 \* 1024 \* 1024`
```

# Creating a space-optimized rollback

## To create a space-optimized rollback

- ◆ To create a space-optimized rollback for a specified file system, enter the following:

```
Storage> rollback create space-optimized rollback_name  
fs_name [cacheobj]
```

`rollback_name`      Indicates the name of the rollback.

`fs_name`            Indicates the name of the file system for which to create the space-optimized rollback.

`cacheobj`          Indicates the cache object name. If the cache object is specified, then the shared cache object is used. Otherwise, Veritas Access automatically creates a cache object for the rollback.

For example:

```
Storage> rollback create space-optimized snap4 fs4  
100%[#] Create rollback
```

# Creating a full-sized rollback

## To create a full-sized rollback for a specified file system

- ◆ To create a Veritas Access full-sized rollback for a specified file system, enter the following:

```
Storage> rollback create full-sized rollback_name  
      fs_name pool
```

`rollback_name`      Indicates the name of the rollback.

`fs_name`            Indicates the name of the file system for which to create the full-sized rollback.

`pool`                Indicates the name of the pool on which to create the full-sized rollback.

The disks used for the rollback are allocated from the specified pool.

For example:

```
Storage> rollback create full-sized snap5 fs4 pool1  
100%[#] Create rollback
```

## Listing Veritas Access instant rollbacks

### To list Veritas Access instant rollbacks

- ◆ To list Veritas Access instant rollbacks, enter the following:

```
Storage> rollback list [fs_name]
```

where *fs\_name* is the name of the file system where you want to list the instant rollbacks.

If no file system is specified, instant rollbacks are displayed for all the file systems.

```
Storage> rollback list
```

NAME	TYPE	FILESYSTEM	SNAPDATE
roll5	fullinst	fs4	2010/10/15 20:04
roll1	spaceopt	bigfs	2010/10/15 17:03

```
Storage> rollback list fs4
```

NAME	TYPE	SNAPDATE	CHANGED_DATA	SYNCED_DATA
roll5	fullinst	2010/10/15 20:04	640K(0.1%)	800M(100%)

## Restoring a file system from an instant rollback

Prior to restoring a file system by a specified rollback, the file system should be offline.

See [“Taking an instant rollback offline”](#) on page 594.

### To restore a file system from an instant rollback

- 1 To restore a file system from an instant rollback, enter the following:

```
Storage> rollback restore fs_name rollback_name
```

`fs_name` Indicates the name of the file system that you want to restore.

`rollback_name` Indicates the name of the rollback that you want to restore.

For example, to restore a file system by a given instant rollback, enter the following:

```
Storage> rollback restore fs4 snap4
```

- 2 Bring the file system back online.

See [“Bringing an instant rollback online”](#) on page 594.

Bringing the file system online may take some time depending on the size of the file system.

## Refreshing an instant rollback from a file system

### To refresh an instant rollback from a file system

- ◆ To refresh an instant rollback from a file system, enter the following:

```
Storage> rollback refresh rollback_name fs_name
```

`rollback_name` Indicates the name of the rollback that you want to refresh.

`fs_name` Indicates the name of the file system that you want to refresh.

For example:

```
Storage> rollback refresh roll15 fs4
ACCESS rollback WARNING V-288-0
rollback roll15 will be refreshed to filesystem fs4
ACCESS rollback
WARNING V-288-0 Are you sure to refresh rollback roll15 with
filesystem fs4? (yes/no) yes
100% [#] Refresh rollback
ACCESS rollback SUCCESS V-288-0 snapshot roll15 refreshed
successfully from fs fs4
```

## Bringing an instant rollback online

You can choose to bring an instant rollback online and use it as a live file system. If the original file system is offline for some reason, the instant rollback can be used as a backup.

When an instant rollback is mounted and written to with new data, the instant rollback may no longer be suitable for use in restoring the contents of the original volume. If you chose to write to an instant rollback, create another instant rollback as a backup of the original file system.

### Bringing an instant rollback online

- ◆ To bring an instant rollback online, enter the following:

```
Storage> rollback online rollback_name
```

*rollback\_name*      Indicates the name of the rollback that you want to bring online.

For example:

```
Storage> rollback online snap1  
Online the filesystem of rollback "snap1"
```

The instant rollback is available for read/write access just as the file system.

## Taking an instant rollback offline

### Taking an instant rollback offline

- ◆ To take an instant rollback offline, enter the following:

```
Storage> rollback offline rollback_name
```

*rollback\_name*      Indicates the name of the rollback that you want to take offline.

For example:

```
Storage> rollback offline snap1  
Offline the filesystem of snapshot "snap1"
```

## Destroying an instant rollback

The instant rollback must be in the offline state before it can be destroyed.

See [“Taking an instant rollback offline”](#) on page 594.

**To destroy an instant rollback**

- ◆ To destroy an instant rollback, enter the following:

```
Storage> rollback destroy rollback_name fs_name
```

*rollback\_name*                    Indicates the name of the rollback that you want to destroy.

*fs\_name*                            Indicates the name of the file system that you want to destroy.

For example:

```
Storage> rollback destroy snap1 myfs2  
Destroy the snapshot "snap1" of filesystem "myfs2"
```

## Creating a shared cache object for Veritas Access instant rollbacks

You can create a shared cache object for Veritas Access instant rollbacks. Space-optimized rollbacks use a storage cache to save the data. Using a shared cache object, cache storage can be shared by all the space-optimized rollbacks.

**To create a shared cache object for Veritas Access instant rollbacks**

- ◆ To create a shared cache object for Veritas Access instant rollbacks, enter the following:

```
Storage> rollback cache create cache_name [cache_size] [pool]
```

<code>cache_name</code>	Indicates the name of the cache object you want to create.
<code>cache_size</code>	<p>Indicates the cache size for the cache object. Cache size can be specified in any units, such as M, G, or T.</p> <p>The size of the shared cache object should be sufficient to record changes to the file system during intervals between instant rollback refreshes. By default, the size of the cache object for an instant rollback is 20% of the total size of the parent file system.</p> <p>The size of the cache object is dependent on your environment.</p>
<code>pool</code>	<p>Indicates the pool for storing the cache object.</p> <p>For better performance, the pool used for the space-optimized rollback should be different from the pool used by the file system.</p>

For example:

```
Storage> rollback cache create mycache 500m pool1
Create a shared cache object "mycache" with the disks from "pool1",
the size is 500m
```

### To convert an existing file system into a cache object

- 1 Select or create a file system with the layout that you want to use for the cache object. In this way, you can create cache objects with any kind of file system type. If you use an existing file system, the data on the file system is lost when you convert it to a cache object.

The following example shows how to create a file system with a file system type of striped:

```
Storage> fs create striped cobj1 100m 2 pool0
100% [#] Creating striped filesystem
```

- 2 Run the `Storage> rollback cache create` command without the `cache_size` and `pool` parameters:

```
Storage> rollback cache create cache_name
```

*cache\_name* is the name of the file system from step 1 that you want to convert.

A confirmation message in the Veritas Access CLI asks if you want to convert the specified file system to a cache object.

For example, to convert the striped file system `cobj1` to a cache object:

```
Storage> rollback cache create cobj1
ACCESS rollback WARNING V-288-0 Filesystem cobj1 will be converted to
cache object.
All data on Filesystem cobj1 will be lost
ACCESS rollback WARNING V-288-0 Are you sure you want to convert cobj1
to a cache object? (yes/no)
yes
100% [#]
```

- 3 Verify that the new cache object exists:

```
Storage> rollback cache list
CACHE NAME      TOTAL (Mb)   USED (Mb) (%)   AVAIL (Mb) (%)   SDCNT
cache1          15           15 (100)         0 (0)             2
cobj1           100          4 (4)            96 (96)           0
```

## Listing cache objects

The `Storage> rollback cache list` command allows you to list the Veritas Access instant rollbacks that are using a cache object.

### To list cache objects for Veritas Access instant rollbacks

- ◆ To list cache objects for Veritas Access instant rollbacks, enter the following:

```
Storage> rollback cache list [cache_name]
```

where *cache\_name* is the name of the cache object you want to display. When *cache\_name* is specified, the instant rollbacks that are using the cache object are listed.

A disabled cache object is listed with '-' as the attribute. *cache2* and *mycache* are in the DISABLED state.

For example:

```
Storage> rollback cache list
CACHE NAME      TOTAL (Mb)    USED (Mb) (%)  AVAIL (Mb) (%)  SDCNT
cache1          15            15 (100)      0 (0)           2
cobj1           100           4 (4)         96 (96)         0
cache2          -             - -           - -             -
mycache         -             - -           - -             -
```

SDCNT is the number of subdisks that have been created on the cache object.

If the cache object is disabled for some reason, it will automatically be restarted when the `Storage> rollback cache list cache_name` command is run.

For example:

```
Storage> rollback cache list cache2
rollbacks located on cache cache2:
roll3
ACCESS rollback WARNING V-288-0 Cache object cache2 was DISABLED,
trying to restart it.
ACCESS rollback INFO V-288-0 Cache object cache2 started successfully.
```

You can choose to start the cache object, or destroy it after destroying all the instant rollbacks located on it.

See [“Destroying a cache object of a Veritas Access instant rollback”](#) on page 599.

If you did not assign a cache object, a cache object is internally created for the instant rollback.

# Destroying a cache object of a Veritas Access instant rollback

## To destroy a cache object of a Veritas Access instant rollback

- ◆ To destroy a cache object of a Veritas Access instant rollback, enter the following:

```
Storage> rollback cache destroy cache_name
```

where *cache\_name* is the name of the cache object that you want to destroy.

For example:

```
Storage> rollback cache destroy mycache
```

You can only destroy the cache object if there is no instant rollback that is using this cache object.

# Configuring NetBackup with Veritas Access

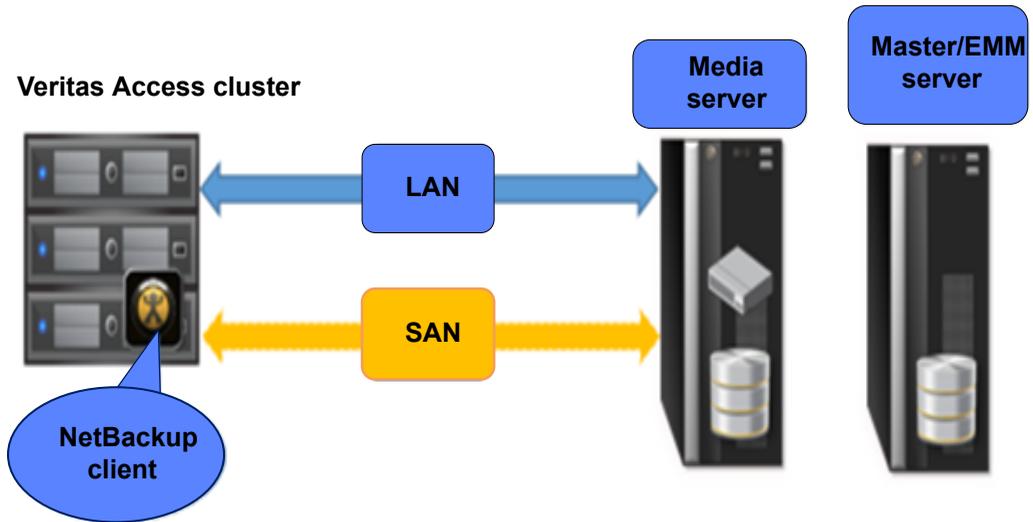
This chapter includes the following topics:

- [About the NetBackup integration with Veritas Access](#)
- [Prerequisites for configuring NetBackup](#)
- [Configuring Veritas Access for NetBackup](#)

## About the NetBackup integration with Veritas Access

Veritas Access is integrated with Veritas NetBackup so that a NetBackup administrator can back up your Veritas Access file systems to NetBackup master or media servers and retain the data as per your company policy. Once data is backed up, a storage administrator can delete unwanted data from Veritas Access. The NetBackup master and media servers run on separate computers from Veritas Access and are licensed separately from Veritas Access.

You configure NetBackup domain information using the Veritas Access CLISH. The Veritas Access CLISH has a dedicated `Backup>` menu. From the `Backup>` menu, register the NetBackup client with the NetBackup domain. Information is saved in the `bp.conf` file on Veritas Access.

**Figure 34-1** Configuration of Veritas Access with NetBackup

Consolidating storage reduces the administrative overhead of backing up and restoring many separate file systems. With a 255 TB maximum file system size, Veritas Access makes it possible to collapse file storage into fewer administrative units, thus reducing the number of backup interfaces and operations. Critical file data can be backed up and restored through the NetBackup client on Veritas Access.

See [“Prerequisites for configuring NetBackup”](#) on page 601.

See [“Configuring Veritas Access for NetBackup”](#) on page 602.

See the *Veritas Access Installation Guide* for the supported NetBackup clients.

See the *Veritas Access Troubleshooting Guide* for setting the NetBackup client log levels and debugging options.

## Prerequisites for configuring NetBackup

Before configuring NetBackup for Veritas Access, you must have completed the following:

- You must have a NetBackup master server external to your Veritas Access cluster. The NetBackup administrator configures the NetBackup master server. See the NetBackup product documentation for more information.
- Add the valid licenses on the NetBackup master server.
- Make sure that the Veritas Access server and the NetBackup server can resolve the host name.

# Configuring Veritas Access for NetBackup

To back up your data with NetBackup, you must register the installed and configured NetBackup master server with Veritas Access.

To configure NetBackup for Veritas Access, perform the following tasks in the order shown:

- |  |   |
|--|---|
| Make sure that the prerequisites are met.  | See <a href="#">“Prerequisites for configuring NetBackup”</a> on page 601.  |
| Register the NetBackup master server.  | See <a href="#">“Registering a NetBackup master server, an EMM server, or adding an optional media server”</a> on page 603. |
| Display the current status of the NetBackup client.  | See <a href="#">“Displaying the status of NetBackup services”</a> on page 604.  |
| Reset the values for the NetBackup master server or the NetBackup EMM server.              | See <a href="#">“Registering a NetBackup master server, an EMM server, or adding an optional media server”</a> on page 603. |
| Display the current status of the NetBackup client.  | See <a href="#">“Displaying the status of NetBackup services”</a> on page 604.  |
| Reset the NetBackup virtual name.  | See <a href="#">“Configuring the virtual name of NetBackup”</a> on page 607.  |
| Register the NetBackup master server with the NetBackup client.                            | See <a href="#">“Registering a NetBackup master server, an EMM server, or adding an optional media server”</a> on page 603. |
| Configure the virtual name that the NetBackup master server uses for the NetBackup client. | See <a href="#">“Configuring the virtual name of NetBackup”</a> on page 607.  |
| Display the current status of the NetBackup client.  | See <a href="#">“Displaying the status of NetBackup services”</a> on page 604.  |
| Verify that Veritas Access is configured with the NetBackup client.                        | See <a href="#">“Displaying the status of NetBackup services”</a> on page 604.  |

- Configure the `/etc/hosts` file to ping the NetBackup master or media server. See [“Configuring DNS in Veritas Access”](#) on page 606.
- Specify the files to back up or restore. See [“Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client”](#) on page 609.
- Specify the snapshot to back up or restore. See [“Performing a backup or restore of a snapshot”](#) on page 610.
- Uninstalling or installing the NetBackup client. See [“Installing or uninstalling the NetBackup client”](#) on page 610.

## Registering a NetBackup master server, an EMM server, or adding an optional media server

You register the NetBackup master server or the EMM server so that it can communicate with Veritas Access. If necessary, you can reset the values of the NetBackup master server or the EMM server to their default configurations. You can optionally add a media server.

The NetBackup EMM server is generally the master server. The NetBackup master server can be the NetBackup media server, but it is not mandatory that the NetBackup master server be the NetBackup media server. In production environments, the NetBackup media server is separate from the NetBackup master server.

See the `backup_netbackup(1)` man page for detailed examples.

### To register the NetBackup master server or the NetBackup EMM server with Veritas Access

- 1 Register the NetBackup master server with Veritas Access.

For a NetBackup master server:

```
Backup> netbackup master-server set server
```

For a NetBackup EMM server:

- 2 Register the NetBackup EMM server with Veritas Access.

```
Backup> netbackup emm-server set server
```

### To reset the value for the NetBackup master server or the NetBackup EMM server

- 1 Reset the value for the NetBackup master server.

For a NetBackup master server:

```
Backup> netbackup master-server reset
```

For a NetBackup EMM server:

- 2 Reset the value for the NetBackup EMM server.

```
Backup> netbackup emm-server reset
```

### To add an optional NetBackup media server

- ◆ Add an optional NetBackup media server.

If the NetBackup master server is also acting as a NetBackup media server, then add the NetBackup media server using the NetBackup master server hostname.

For example:

```
Backup> netbackup media-server add FQDN of master server
```

### To delete an already configured NetBackup media server

- ◆ Delete an already configured NetBackup media server.

```
Backup> netbackup media-server delete server
```

## Displaying the status of NetBackup services

Use the backup commands to display the status of the NetBackup services.

See the following man pages for detailed examples:

- `backup_show(1)`
- `backup_status(1)`
- `backup_start(1)`
- `baclup_stop(1)`

### To display NetBackup services

- ◆ Display the current NetBackup services.

```
Backup> show
```

#### Example:

```
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): nbumaster.veritas.com
Backup Device:        pubeth1
```

If the settings were configured while the backup and the restore services were online, they may not be in use by Veritas Access. To display all of the configured settings, first run the `Backup> stop` command, then run the `Backup> start` command.

### To display the status of backup services

- ◆ Display the status of backup services.

```
Backup> status
```

#### Example:

```
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.
```

If the NetBackup server is started and online, then `Backup> status` displays any on-going backup or restore jobs.

### To start or stop backup services

- 1 Start the backup services.

```
Backup> start [nodename]
```

You can also change the status of a virtual IP address to online after it has been configured using the `Backup> virtual-ip` command. This command applies to any currently active node in the cluster that handles backup and restore jobs.

See [“Configuring or changing the virtual IP address used by NetBackup”](#) on page 606.

- 2 Stop the backup services.

```
Backup> stop
```

You can also change the status of a virtual IP address to offline after it has been configured using the `Backup> virtual-ip` command.

See [“Configuring or changing the virtual IP address used by NetBackup”](#) on page 606.

The `Backup> stop` command does nothing if any backup jobs are online that involve Veritas Access file systems.

## Configuring DNS in Veritas Access

We recommend that you configure DNS in Veritas Access. After configuring DNS, Veritas Access should be able to resolve the fully qualified domain name of the NetBackup master or media server from DNS.

### To add DNS in Veritas Access

- ◆ Configure DNS using the CLI.

```
Network> dns set
```

## Configuring or changing the virtual IP address used by NetBackup

You can configure or change the virtual IP address of NetBackup. This address is a highly-available virtual IP address in the cluster.

---

**Note:** Configure the virtual IP address using the `Backup> virtual-ip` command so that it is different from all of the virtual IP addresses, including the Console server IP address and the physical IP addresses that are used to install Veritas Access. Use the `Network> ip addr show` command to display the currently assigned virtual IP addresses on Veritas Access.

---

See the `backup_virtual-ip(1)` man page for detailed examples.

### To configure or change the virtual IP address used by NetBackup

- ◆ Configure or change the virtual IP address of NetBackup on Veritas Access.

```
Backup> virtual-ip ipaddr [device]
```

See [“Configuring the virtual name of NetBackup”](#) on page 607.

## Configuring the virtual name of NetBackup

You can either configure the virtual name for the NetBackup master server, or you can reset the value to its default or unconfigured state.

See the `backup_virtual-name(1)` man page for detailed examples.

### To set or reset the NetBackup virtual name

- ◆ Set or reset the NetBackup virtual name.

For setting the virtual name:

```
Backup> virtual-name set name
```

For resetting the virtual name:

```
Backup> virtual-name reset
```

Make sure that *name* can be resolved through DNS, and its IP address can be resolved back to *name* through the DNS reverse lookup. Also, make sure that *name* resolves to an IP address that is configured by using the `Backup> virtual-ip` command.

See [“Configuring or changing the virtual IP address used by NetBackup”](#) on page 606.

## Adding or deleting patterns to the list of files in backups

You can add or delete specified patterns to or from the files that you want to include or exclude from NetBackup backups. For example, you can create a backup policy

with different patterns such that only `.gif` files are backed up and `.iso` files are excluded.

See the `backup_netbackup(1)` man page for detailed examples.

#### To add or delete the given pattern to the list of files included for backup

- ◆ Add the specified pattern to the files that are included for backup.

For adding specified patterns to included files:

```
Backup> netbackup include_list add pattern [policy] [schedule]
```

For deleting specified patterns from included files:

```
Backup> netbackup include_list delete pattern [policy] [schedule]
```

#### To add or delete a given pattern to the list of files excluded from backup

- ◆ Add a given pattern to the list of files that are excluded from backup.

For adding a given pattern to excluded files:

```
Backup> netbackup exclude_list add pattern [policy] [schedule]
```

For deleting the given pattern from excluded files:

```
Backup> netbackup exclude_list delete pattern [policy] [schedule]
```

## Displaying the included and excluded files for backups

You can specify a policy pattern that lets you specify which files to include or exclude from NetBackup backups. For example, you can specify that only `.gif` files are backed up, and `.iso` files are excluded. You can then display those files.

See the `backup_netbackup(1)` man page for detailed examples.

#### To display files included or excluded for backups

- ◆ Display the files that are included or excluded for backups.

For included files:

```
Backup> netbackup include_list show [policy] [schedule]
```

For excluded files:

```
Backup> netbackup exclude_list show [policy] [schedule]
```

## Performing a backup or restore of a Veritas Access file system over a NetBackup SAN client

You can perform a backup or restore of a Veritas Access file system over a NetBackup SAN client. A NetBackup SAN client is a NetBackup client for which Fibre Transport services are activated.

Backup and restore operations are done on the NetBackup master server by a NetBackup administrator using the NetBackup Administration Console. If the NetBackup master server can connect to the NetBackup client on Veritas Access, the NetBackup master server starts the backup or restore operations.

Before performing a backup or restoration of a Veritas Access file system over a NetBackup SAN client, do the following:

- Verify that the virtual IP address is online.
- Verify that the NetBackup client state is online.
- Configure the Fibre Transport media server.  
See the *Veritas NetBackup SAN client and Fibre Transport Guide* for more information on configuring the NetBackup Fibre Transport media server.

See the `backup(1)` man page for detailed examples.

### To perform a backup of a file system over a NetBackup SAN client

- 1 Check the status of the NetBackup client.

```
Backup> status
```

- 2 Enable the SAN client from the CLI.

```
Backup> netbackup sanclient enable
```

- 3 Verify if the SAN client has been enabled or not from the CLI.

```
Backup> status
```

- 4 Using the NetBackup Administration Console, start a backup operation.

**To perform a restore of a file system over a NetBackup SAN client**

- 1 Check the status of the NetBackup client.

```
Backup> status
```

- 2 Using the NetBackup Administration Console, start a restore operation.
- 3 Check the status of the NetBackup client.

```
Backup> status
```

## Performing a backup or restore of a snapshot

Using the NetBackup Administration Console, a NetBackup administrator can perform a backup or restore of a snapshot.

Veritas Access as a NetBackup client supports the VxFS\_Checkpoint snapshot method. See the *Veritas NetBackup Snapshot Client Administrator's Guide* for more information on configuring snapshot policies.

**To perform a backup of a snapshot**

- ◆ Using the NetBackup Administration Console, start a snapshot backup.  
The snapshot triggered by the NetBackup job can be seen from the CLI.

```
Storage> snapshot list
```

**To perform a restore of a snapshot**

- 1 Using the NetBackup Administration Console, navigate to **Backup, Archive, and Restore**.
- 2 Click the **Restore Files** tab.
- 3 Click the **Restore** option.
- 4 Specify the directory location for performing the restore operation.

```
/vx/name_of_file_system/Restores
```

## Installing or uninstalling the NetBackup client

The NetBackup master server version should be higher or equal to the NetBackup client version. To upgrade the NetBackup client, uninstall the currently installed version of the NetBackup client and then install the specified version of the NetBackup client. The uninstall command runs on all the nodes of the Veritas Access cluster.

Veritas Access supports two major versions of the NetBackup client, version 7.6 and 7.7. By default, Veritas Access comes with the 7.7 version of the NetBackup client.

See the `backup(1)` man page for detailed examples.

## To install the NetBackup client

- 1 Display the currently installed version of the NetBackup client.

```
Backup> show
```

- 2 Install the specified NetBackup client.

```
Backup> install version [URL]
```

You must specify the version of the NetBackup client that you want to install. If you do not specify a URL, the `Backup> install` command has the information on the file system for the location it needs. Specify the major release version (7.7 or 7.6) as the second parameter. You can specify the NetBackup package minor release or patches (7.7.1 for a 7.7 major release) as the third parameter to install.

If the base NetBackup client version is 7.6.

```
Backup> install 7.6 scp://support@192.168.2.10:/home/NetBackup_7.6_
CLIENTS2.tar.gz
```

If the base NetBackup client version is 7.7.

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7_
CLIENTS2.tar.gz
```

If there are minor releases or patches from the NetBackup client.

```
Backup> install 7.6 scp://support@192.168.2.10:/home/NetBackup_7.6.0.1_
CLIENTS2.tar.gz
```

```
Backup> install 7.7 scp://support@192.168.2.10:/home/NetBackup_7.7.1_
CLIENTS2.tar.gz
```

For example, consider that the NetBackup client binaries are placed on the following host:

```
192.168.2.10
```

```
Backup> install 7.6 scp://support@192.168.2.10:/home/NetBackup_7.6.0.1_
CLIENTS2.tar.gz
```

Where 192.168.2.10 is the host IP address on which the NetBackup client packages are placed.

```
NetBackup_7.6.0.1_CLIENTS2.tar.gz
```

This is the NetBackup client package.

- 3 Double check if the Red Hat compatible NetBackup client is available in this package.

```
support:  
system user and specify password when prompted.
```

- 4 Verify that the specified NetBackup client is installed.

```
Backup> show
```

### **To uninstall the NetBackup client**

- 1 Display the currently installed version of the NetBackup client.

```
Backup> show
```

- 2 Uninstall the existing version of the NetBackup client.

```
Backup> uninstall
```

- 3 Display the current running version of the NetBackup client.

```
Backup> show
```

- 4 Verify that the NetBackup client is not installed.

```
Backup> show
```

# Reference

- [Appendix A. Veritas Access documentation](#)

# Veritas Access documentation

This appendix includes the following topics:

- [Using the Veritas Access product documentation](#)
- [About accessing the online man pages](#)

## Using the Veritas Access product documentation

The latest version of the Veritas Access product documentation is available on the Veritas Services and Operations Readiness Tools (SORT) website.

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

You need to specify the product and the platform and apply other filters for finding the appropriate document.

Make sure that you are using the current version of documentation. The document version appears on page 2 of each guide. The publication date appears on the title page of each document. The documents are updated periodically for errors or corrections.

See the *Veritas Access Release Notes* for information on documentation changes in this release.

The following documents are available on the SORT site:

- *Veritas Access Command-Line Administrator's Guide*
- *Veritas Access Installation Guide*
- *Veritas Access Quick Start Guide*
- *Veritas Access Release Notes*

- *Veritas Access Third-Party License Agreements*
- *Veritas Access Troubleshooting Guide*

## 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 `Network> man ldap command`.

```
Network> man ldap
```

```
NAME
```

```
ldap - configure LDAP client for authentication
```

```
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}
```

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 will 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: `exit`.

For example:

```
ACCESS.Admin> exit
```

```
ACCESS>
```

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

For example:

```
ACCESS> logout
```

# Index

## A

### about

- Active Directory (AD) 161
- bonding Ethernet interfaces 37
- changing share properties 428
- configuring CIFS for AD domain mode 166
- configuring routing tables 67
- configuring the policy of each tiered file system 485
- configuring Veritas Access for CIFS 156
- configuring Veritas Access to use jumbo frames 54
- creating and maintaining file systems 334
- data deduplication 441
- Ethernet interfaces 48
- FTP 239
- FTP local user set 251
- FTP set 242
- I/O fencing 110
- iSCSI 117
- job failover and failback 570
- leaving AD domain 171
- load balancing for the normal clustering mode 211
- locally saved configuration files 313
- managing bandwidth limits 538
- managing CIFS shares 421
- managing home directories 204
- NFS file sharing 404
- reconfiguring CIFS service 197
- scale-out file systems 335
- setting NTLM 175
- setting trusted domains 176
- shares 398
- snapshot schedules 582
- snapshots 574
- storage provisioning and management 93
- storing account information 193
- striping file systems 340
- the IP addresses for the Ethernet interfaces 47
- Veritas Access file-level replication 522

### accessing

- man pages 616
- replication destinations 568
- Veritas Access product documentation 615

accessing Veritas Access Replication commands 523

### Active Directory

- setting the trusted domains for 192

### Active Directory (AD)

- about 161
- joining Veritas Access to 164
- verifying Veritas Access has joined successfully 166

### AD domain mode

- changing domain settings 171
- configuring CIFS 166
- security settings 171
- setting domain 167
- setting domain user 167
- setting security 167
- starting CIFS server 167

### AD interface

- using 174

### AD trusted domains

- disabling 192

### add local user

- FTP 249

### adding

- a column to a file system 355
- a column to a tiered file system 480
- a severity level to an email group 296
- a syslog server 301
- an email address to a group 296
- an email group 296
- CIFS share 428
- disks 98
- external NetBackup master server to work with Veritas Access 603
- filter to a group 296
- IP address to a cluster 48
- Master, System Administrator, and Storage Administrator users 24
- mirror to a file system 353

- adding *(continued)*
  - mirror to a tier of a file system 481
  - mirrored tier to a file system 478
  - mirrored-striped tier to a file system 478
  - NetBackup Enterprise Media Manager (EMM) server 603
  - NetBackup media server 603
  - OpenStack Manila driver 276
  - second tier to a file system 478
  - SNMP management server 304
  - striped tier to a file system 478
  - striped-mirror tier to a file system 478
  - users 24
    - naming requirements for 27
  - VLAN interfaces 57
- adding a mapping
  - between CIFS and NFS users 203
- adding and configuring
  - Veritas Access to the Kerberos realm 152
- adding or deleting patterns
  - included in the list of files for backups 607
- aio\_fork option
  - setting 224
- alerts
  - file system removing 392
- allowing
  - metadata information to be written on the secondary tier 494
  - specified users and groups access to the CIFS share 432
- application performance during replication 538
- authenticating
  - NFS clients using Kerberos 151
- authentication
  - configuring the LDAP client using the CLI 191
- B**
- back up
  - Veritas Access file system over a SAN client 609
- backup or restore
  - NetBackup snapshot 610
- backup services
  - displaying the status of 604
  - starting 604
  - stopping 604
- bandwidth limit
  - throttling 538
- best practices
  - creating file systems 337
- best practices *(continued)*
  - for using the Veritas Access deduplication feature 444
    - setting relocation policies 489
- bind distinguished name
  - setting for LDAP server 75
- bonding
  - Ethernet interfaces 39
- bonding Ethernet interfaces
  - about 37
- bringing
  - file system online or offline 350
- buckets and objects
  - creating 237
- C**
- cache area
  - monitoring 517
  - verifying 517
- Cache behavior
  - customizing 514
- cache object
  - destroying for an instant rollback 599
- cache objects
  - listing 597
- caching mode
  - setting 520
- caching VxFS in read mode 511
- caching VxFS in write mode 513
- certificate of the REST server
  - set 272
- changing
  - an IP address to online
    - on any running node 48
  - configuration of an Ethernet interface 56
  - DMP I/O policy 318
  - domain settings for AD domain mode 171
  - local CIFS user password 225
  - NFS daemons 318
  - ninodes cache size 318
  - security settings 161
  - security settings after CIFS server is stopped 161
  - share properties about 428
- changing the caching mode 520
- checking
  - and repairing a file system 384
  - for stale mirrors on file systems 387
  - I/O fencing status 111
  - on the status of the NFS server 146

- CIFS
  - allowing specified users and groups access to the CIFS share 432
  - configuring schema extensions 186
  - denying specified users and groups access to the CIFS share 433
  - export options 424
  - mapuser commands 202
  - standalone mode 157
  - using multi-domain controller support 170
- CIFS aio\_fork option
  - setting 224
- CIFS and NFS protocols
  - share directories 400
- CIFS clustering modes
  - about 156
  - switching from ctdb to normal 215
  - switching from normal to ctdb 212
- CIFS data migration
  - enabling 228
- CIFS home directories
  - displaying the quota values for 377
  - quotas 368
  - using quotas for 370
- CIFS operating modes
  - about 156
- CIFS server
  - changing security settings after stopped 161
  - configuring with the LDAP backend 191
  - starting 198
  - trusted domains that are allowed access 177
- CIFS server status
  - standalone mode 158
- CIFS service
  - standalone mode 158
- CIFS share
  - adding 428
  - deleting 434
  - exporting as a directory 421
  - exporting the same file system/directory as a different CIFS share 423
  - making shadow copy aware 436
  - modifying 435
- CIFS share and home directory
  - migrating from ctdb to normal clustering mode 220
- CIFS shares and home directories
  - migrating from ctdb clustering modes 216
- CIFS shares and home directories *(continued)*
  - migrating from normal to ctdb clustering mode 218
- CIFS snapshot
  - exporting 434
- CIFS/NFS sharing
  - mapping user names 200
- clearing
  - DNS domain names 44
  - DNS name servers 44
  - LDAP configured settings 75
- client configurations
  - displaying 79
  - LDAP server 79
- cloud tier
  - obtaining data usage statistics 507
- cluster
  - adding an IP address to 48
  - changing an IP address to online for any running node 48
  - displaying all the IP addresses for 48
- clustering modes
  - ctdb 210
- clusters
  - FSS 94
- columns
  - adding or removing 355
  - adding or removing from a tiered file system 480
- command history
  - displaying 28
- Command-Line Interface (CLI)
  - getting help on how to use 30
- communicating
  - source and destination clusters 528
- concurrent access
  - object access service 403
  - S3 235
- configuration
  - of an Ethernet interface
    - changing 56
- configuration files
  - deleting the locally saved 315
  - viewing locally saved 315
- configuration settings
  - exporting either locally or remotely 315
  - importing either locally or remotely 315
- configuring
  - AD schema with CIFS-schema extensions 186
  - bandwidth limit 538

- configuring (*continued*)
    - CIFS for standalone mode 157
    - CIFS server with the LDAP backend 191
    - DNS 606
    - event notifications 295
    - IP routing 68
    - iSCSI devices 119
    - iSCSI discovery 121
    - iSCSI initiator 118
    - iSCSI initiator name 118
    - iSCSI targets 127
    - job resynchronization 567
    - NetBackup virtual IP address 606
    - NetBackup virtual name 607
    - netgroups 414
    - NFS client for ID mapping 150
    - NIC devices 59
    - NSS lookup order 83
    - OpenStack Cinder 261
    - the policy of each tiered file system 485
    - Veritas Access for CIFS 156
    - Veritas Access to work with OpenStack Manila 269
    - VLAN interfaces 57
    - Windows Active Directory as an IDMAP backend 185
  - configuring and managing
    - storage pools for the OpenStack Manila user 275
  - configuring CIFS share
    - secondary storage for an Enterprise Vault store 422
  - configuring Ethernet interfaces
    - about 48
  - configuring NetBackup
    - prerequisites 601
  - configuring routing tables
    - about 67
  - configuring the cloud as a tier feature
    - scale-out file systems 497
  - configuring Veritas Access to use jumbo frames
    - about 54
  - converting
    - existing file system into a cache object 595
  - coordinating
    - cluster nodes to work with NTP servers 85
  - coordinator disks
    - replacing 111
  - creating
    - buckets and objects 237
  - creating (*continued*)
    - full-sized rollback 591
    - local CIFS group 227
    - local CIFS user 225
    - mirrored file systems 346
    - mirrored-stripe file systems 346
    - OpenStack Manila file share 281
    - OpenStack Manila share snapshot 284
    - OpenStack Manila share type 280
    - RPO report 569
    - share backend on the OpenStack controller node 277
    - shared cache object 595
    - simple file systems 346
    - snapshot schedules 583
    - snapshots 575
    - space-optimized instant rollbacks 590
    - storage pools 105
    - striped file systems 346
    - striped-mirror file systems 346
  - creating account
    - S3 236
  - creating an OpenStack Manila share
    - from an OpenStack Manila snapshot 284
  - creating and maintaining file systems
    - about 334
  - creating and scheduling a policy
    - scale-out file system 505
  - creating file systems
    - best practices 337
  - ctdb clustering mode
    - about 210
    - directory-level share support 421
    - load balancing 212
    - switching the clustering mode 212
  - current Ethernet interfaces and states
    - displaying 55
  - current users
    - displaying list 24
- ## D
- data deduplication
    - about 441
  - decreasing
    - size of a file system 358
  - deduplication
    - use-cases 442
  - deduplication scenario
    - end-to-end 445

- deduplication workflow
  - overview 443
- default
  - passwords
    - resetting Master, System Administrator, and Storage Administrator users 24
- defining
  - what to replicate 553
- defrag 379
- defragmenting
  - file systems 379
- delete local user
  - FTP 249
- deleting
  - already configured SNMP management server 304
  - CIFS share 434
  - configured mail server 296
  - configured NetBackup media server 603
  - email address from a specified group 296
  - email groups 296
  - filter from a specified group 296
  - home directories 209
  - home directory of given user 209
  - local CIFS group 227
  - local CIFS user 225
  - locally saved configuration file 315
  - NFS options 417
  - route entries from routing tables of nodes in cluster 68
  - severity from a specified group 296
  - snapshot schedules 586
  - syslog server 301
  - users 24
  - VLAN interfaces 57
- denying
  - specified users and groups access to the CIFS share 433
- description of Veritas Access Replication 523
- destroying
  - a file system 393
  - cache object of an instant rollback 599
  - I/O fencing 111
  - instant rollbacks 594
  - snapshots 578
  - storage pools 105
- directories
  - displaying exported 413
  - unexporting the share 417
- directory-level share support
  - ctdb clustering mode 421
- disabling
  - AD trusted domains 192
  - creation of home directories 209
  - DNS settings 44
  - FastResync option 386
  - I/O fencing 111
  - LDAP clients
    - configurations 79
  - NIS clients 81
  - NTLM 175
  - NTP server 85
  - quota limits used by snapshots 578
- disk
  - formatting 101
  - removing 101
- disk layout versions
  - upgrading 394
- disks
  - adding 98
  - removing 98
- displaying
  - all the IP addresses for cluster 48
  - command history 28
  - current Ethernet interfaces and states 55
  - current list of SNMP management servers 304
  - DMP I/O policy 318
  - DNS settings 44
  - events on the console 303
  - existing email groups or details 296
  - exported directories 413
  - file system alert values 392
  - file system I/O statistics 312
  - file systems that can be exported 405
  - files moved or pruned by running a policy 493
  - home directory usage information 208
  - included files for backups 608
  - information for all disk devices for the nodes in a cluster 95
  - LDAP client configurations 79
  - LDAP configured settings 75
  - list of current users 24
  - list of SmartTier systems 484
  - list of syslog servers 301
  - local CIFS group 227
  - local CIFS user 225
  - NetBackup configurations 604
  - network configuration and statistics 35

- displaying (*continued*)
  - NFS daemons 318
  - NFS statistics 147
  - ninodes cache size 318
  - NIS-related settings 81
  - NSS configuration 83
  - option tunefstab 318
  - policy of each tiered file system 486
  - routing tables of the nodes in the cluster 68
  - schedules for tiered file systems 491
  - share properties 431
  - snapshot quotes 578
  - snapshot schedules 585
  - snapshots 576
  - snapshots that can be exported 405
  - status of backup services 604
  - status of the NTP server 85
  - system date and time 89
  - system statistics 310
  - tier location of a specified file 484
  - time interval or number of duplicate events for notifications 307
  - values of the configured SNMP notifications 304
  - values of the configured syslog server 301
  - VLAN interfaces 57
  - volpagemod\_max\_memsz parameter of vxtune 325
- displaying a mapping
  - between CIFS and NFS users 203
- displaying WWN information 102
- DMP I/O policy
  - changing 318
  - displaying 318
  - resetting 318
- DNS
  - configuring 606
  - domain names
    - clearing 44
  - name servers
    - clearing 44
    - specifying 44
  - settings
    - disabling 44
    - displaying 44
    - enabling 44
- domain
  - setting 198
  - setting user name 198
- domain controller
  - setting 198
- domain name
  - for the DNS server
    - setting 44
- E**
  - email address
    - adding to a group 296
    - deleting from a specified group 296
  - email groups
    - adding 296
    - deleting 296
    - displaying existing and details 296
  - enable or disable
    - SSL status of the REST server 272
  - enabling
    - CIFS data migration 228
    - DNS settings 44
    - FastResync for a file system 385
    - I/O fencing 111
    - LDAP client configurations 79
    - NIS settings 81
    - NTLM 175
    - NTP server 85
    - quota limits used by snapshots 578
  - enabling, disabling, and displaying
    - file system quotas 361
  - Enterprise Vault store
    - configuring CIFS share as secondary storage 422
  - Ethernet interfaces
    - bonding 39
    - changing configuration of 56
  - event notifications
    - configuring 295
    - displaying time interval for 307
  - event reporting
    - setting events for 307
  - events
    - displaying on the console 303
  - excluded files
    - displaying 608
  - excluding directories and files
    - setting up 546
  - export options
    - CIFS 424
  - exporting
    - an NFS share 405
    - CIFS snapshot 434

- exporting *(continued)*
  - configuration settings 315
  - directory as a CIFS share 421
  - events in syslog format to a given URL 309
  - NFS snapshot 417
  - same file system/directory as a different CIFS share 423
  - SNMP MIB file to a given URL 304
- exporting for Kerberos authentication
  - NFS share 410

## F

- failover 452
  - limiting bandwidth 538
- failover and failback
  - about 570
- file system
  - converting into a cache object 595
  - S3 231
- file system alert values
  - displaying 392
- file system alerts
  - removing 392
  - setting 389
- file system I/O statistics
  - displaying 312
- file system quotas
  - enabling, disabling, and displaying 361
  - setting and displaying 363
- file systems
  - adding a mirror to 353
  - bringing online or offline 350
  - checking and repairing 384
  - checking for stale mirrors 387
  - creating 346
  - decreasing the size of 358
  - defragmenting 379
  - destroying 393
  - disabling FastResync option 386
  - enabling FastResync 385
  - increasing the size of 356
  - listing with associated information 352
  - removing a mirror from 353
  - restoring from an instant rollback 592
  - SmartTier
    - displaying 484
  - that can be exported
    - displayed 405
  - types of layout 339
- filter
  - about 296
  - adding to a group 296
  - deleting from a specified group 296
- forcefully
  - importing new LUNs for new or existing pools 104
- formatting
  - a disk 101
- freelist
  - modifying amount of time unused inode spends 326
- FSS
  - functionality 94
  - limitations 95
- FTP
  - about 239
  - add local user 249
  - delete local user 249
  - implementing command changes 244
  - local user password 249
  - local user set download bandwidth 253
  - local user set home directory 253
  - local user set maximum connections 253
  - local user set maximum disk usage 253
  - local user set maximum files 253
  - local user set upload bandwidth 253
  - logupload 249
  - server start 241
  - server status 241
  - server stop 241
  - session show 247
  - session showdetail 247
  - session terminate 247
  - set allow delete 244
  - set anonymous login 244
  - set anonymous logon 244
  - set anonymous write 244
  - set home directory path 244
  - set listen ipv6 244
  - set listen port 244
  - set maximum connections per client 244
  - set non-secure logins 244
  - set security 244
  - show local users 249
- FTP local user set
  - about 251
- FTP set
  - about 242

**G**

group membership  
managing 225

**H**

hiding  
system files when adding a CIFS normal  
share 429

history command  
using 28

home directories  
setting up 206

home directory file systems  
setting 204

home directory of given user  
deleting 209

home directory usage information  
displaying 208

hostname or IP address  
setting for LDAP server 75

how to use  
Command-Line Interface (CLI) 30

**I**

I/O fencing  
about 110  
checking status 111  
destroying 111  
disabling 111  
enabling 111

implementing  
FTP command changes 244

importing  
configuration settings 315  
new LUNs forcefully for new or existing pools 104

included files  
for backups 608

increasing  
LUN storage capacity 100  
size of a file system 356

initiating host discovery of LUNs 104

installing  
NetBackup client 610

instant rollbacks  
about 588  
bringing online 594  
creating a shared cache object 595  
creating full-sized 591

instant rollbacks (*continued*)  
creating space-optimized 590  
destroying 594  
listing 592  
refreshing from a file system 593  
restoring a file system from 592  
taking offline 594

integration with Veritas Access  
NetBackup 600

IP addresses  
adding to a cluster 48  
displaying for the cluster 48  
modifying 48  
removing from the cluster 48

IP addresses for the Ethernet interfaces  
about 47

IP routing  
configuring 68

iSCSI  
about 117

iSCSI devices  
configuring 119

iSCSI discovery  
configuring 121

iSCSI initiator  
configuring 118

iSCSI initiator name  
configuring 118

iSCSI targets  
configuring 127

**J**

job failover and fallback  
about 570

job resynchronization  
configuring 567

joining  
Veritas Access to Active Directory (AD) 164

**K**

Kerberos authentication  
authenticating NFS clients 151

Kerberos realm  
adding and configuring Veritas Access for 152

Kerberos share  
mounting from the NFS client 411

**L**

- layouts
    - types of file system 339
  - LDAP
    - before configuring 74
  - LDAP client
    - configuring for authentication using the CLI 191
  - LDAP password hash algorithm
    - setting password for 75
  - LDAP server
    - clearing configured settings 75
    - disabling client configurations 79
    - displaying client configurations 79
    - displaying configured settings 75
    - enabling client configurations 79
    - setting over SSL 75
    - setting port number 75
    - setting the base distinguished name 75
    - setting the bind distinguished name 75
    - setting the hostname or IP address 75
    - setting the password hash algorithm 75
    - setting the root bind DN 75
    - setting the users, groups, and netgroups base DN 75
  - leaving
    - AD domain 171
  - Limitations
    - S3 233
  - list of SmartTier file systems
    - displaying 484
  - listing
    - all file systems and associated information 352
    - all of the files on the specified tier 483
    - cache objects 597
    - free space for storage pools 105
    - instant rollbacks 592
    - storage pools 105
  - load balancing
    - ctdb clustering mode 212
  - Loading files to the cache 514
  - local CIFS groups
    - creating 227
    - deleting 227
    - displaying 227
    - managing 227
  - local CIFS user
    - creating 225
    - deleting 225
    - displaying 225
  - local CIFS user password
    - changing 225
  - local user and groups
    - managing 224
  - local user password
    - FTP 249
  - local user set download bandwidth
    - FTP 253
  - local user set home directory
    - FTP 253
  - local user set maximum connections
    - FTP 253
  - local user set maximum disk usage
    - FTP 253
  - local user set maximum files
    - FTP 253
  - local user set upload bandwidth
    - FTP 253
  - locally saved configuration files
    - about 313
  - logging
    - on to Veritas Access 23
  - logupload
    - FTP 249
  - LUN storage capacity
    - increasing 100
  - LUNs
    - initiating host discovery 104
- 
- M**
  - mail server
    - deleting the configured mail server 296
    - obtaining details for 296
    - setting the details of external 296
  - man pages
    - how to access 616
  - managing
    - CIFS shares 421
    - group membership 225
    - home directories 204
    - local CIFS groups 227
    - local users and groups 224
  - managing NFS shares
    - using netgroups 414
  - mapping
    - of UNIX users from LDAP to Windows users 204
  - mapuser commands
    - about 202

- Master, System Administrator, and Storage
  - Administrator users
    - adding 24
- maximum number
  - parallel replication jobs 557
- metadata information
  - allowing to be written on the secondary tier 494
  - restricting to the primary tier only 495
- migrating
  - CIFS share and home directory from ctdb to
    - normal clustering mode 220
  - CIFS shares and home directories 216
  - CIFS shares and home directories from normal
    - to ctdb clustering mode 218
- mirrored file systems
  - creating 346
- mirrored tier
  - adding to a file system 478
- mirrored-stripe file systems
  - creating 346
- mirrored-striped tier
  - adding to a file system 478
- modifying
  - an IP address 48
  - CIFS share 435
  - option tunefstab 318
  - policy of a tiered file system 486
  - schedule of a tiered file system 491
  - snapshot schedules 585
  - tunables for iSCSI 132
  - volpagemod\_max\_memsz parameter of
    - vxtune 325
- modifying time
  - unused inode spends on a freelist 326
- monitoring
  - NIC devices using IP addresses 62
- more command
  - using 29
- mounting
  - NFS share from the NFS client 411
- mounting snapshots 580
- moving disks
  - from one storage pool to another 98
- moving files between tiers
  - scale-out file system 498
- multipart uploading
  - S3 234

## N

- naming requirements for
  - adding users 27
- NetBackup
  - configuring NetBackup virtual IP address 606
  - configuring virtual name 607
  - displaying configurations 604
  - integration with Veritas Access 600
- NetBackup EMM server. *See* NetBackup Enterprise Media Manager (EMM) server
- NetBackup Enterprise Media Manager (EMM) server
  - adding to work with Veritas Access 603
- NetBackup master server
  - configuring to work with Veritas Access 603
- NetBackup media server
  - adding 603
  - deleting 603
- NetBackup snapshot
  - backup or restore 610
- netgroups
  - configuring 414
- network
  - configuration and statistics 35
- network interfaces
  - swapping 63
- NFS client
  - configuring for IP mapping 150
- NFS daemons
  - changing 318
  - displaying 318
- NFS file sharing
  - about 404
- NFS options
  - deleting 417
- NFS server
  - checking on the status 146
  - starting 146
  - stopping 146
- NFS share
  - exporting 405
  - exporting for Kerberos authentication 410
- NFS shares
  - managing using netgroups 414
- NFS snapshot
  - exporting 417
- NFS statistics
  - displaying 147
  - resetting 147

- NFS-Ganesha version 3 and version 4
    - recommended tuning parameters 143
  - NIC devices
    - configuring 59
    - monitoring using IP addresses 62
  - ninodes cache size
    - changing 318
    - displaying 318
  - NIS
    - clients
      - disabling 81
      - enabling 81
    - domain name
      - setting on all the nodes of cluster 81
    - related settings
      - displaying 81
    - server name
      - setting on all the nodes of cluster 81
  - nocache caching mode 520
  - node
    - in a cluster
      - displaying information for all disk devices 95
  - node or storage connection failures
    - when using Oracle Direct NFS 289
  - normal clustering mode
    - load balancing 211
  - NSS
    - displaying configuration 83
    - lookup order
      - configuring 83
  - NTLM
    - disabling 175
    - enabling 175
  - NTP server
    - coordinating cluster nodes to work with 85
    - disabling 85
    - displaying the status of 85
    - enabling 85
- O**
- Object access service 230, 438
    - ACL 232
    - concurrent access 235
    - creating S3 accounts 236
    - file system hierarchy 231
    - limitations 233
    - managing 235
    - multipart uploading 234
    - objects and buckets 234
  - Object access service (*continued*)
    - SSL limitations 235
  - objects and buckets
    - S3 234
  - obtaining
    - details of the configured email server 296
  - offline
    - taking an instant rollback offline 594
  - online
    - bringing an instant rollback online 594
  - OpenStack Cinder
    - configuring 261
  - OpenStack Manila
    - integration with Veritas Access 266
  - OpenStack Manila driver
    - adding 276
    - restarting on the OpenStack controller node 278
  - OpenStack Manila file share
    - creating 281
  - OpenStack Manila service
    - start, stop, or display 273
  - OpenStack Manila share snapshot
    - creating 284
    - creating an OpenStack Manila share from 284
  - OpenStack Manila share type
    - creating 280
  - option tuneftab
    - displaying 318
    - modifying 318
  - Oracle Direct NFS
    - node or storage connection failures 289
  - overview
    - deduplication workflow 443
- P**
- password
    - change user password of the REST server 273
    - changing a user's password 24
  - patterns
    - adding or deleting from the list of files included
      - in backups 607
  - performance during replication 538
  - physical and logical data on a file system 442
  - Pinning files to the cache 514
  - planned failback
    - process overview 572
  - planned failover
    - process overview 571

- policies
    - about 484
    - displaying files moved or pruned by running 493
    - displaying for each tiered file system 486
    - modifying for a tiered file system 486
    - relocating from a tiered file system 490
    - removing from a tiered file system 486
    - running for a tiered file system 486
  - prerequisites
    - configuring NetBackup 601
  - preserving
    - snapshot schedules 586
  - private NIC bonding
    - hub 42
    - switch 42
  - privileges
    - about 27
- ## Q
- quota commands
    - setting and displaying file system quotas 363
  - quota limits
    - enabling or disabling snapshot 578
  - quotas
    - CIFS home directories 368
    - displaying the quota values for CIFS home directories 377
    - setting user quotas for users of specified groups 367
    - using for CIFS home directories 370
- ## R
- read caching 510
  - read caching mode 520
  - recommended tuning parameters
    - NFS-Ganesha version 3 and version 4 143
  - reconfiguring CIFS service
    - about 197
  - refreshing
    - instant rollbacks from a file system 593
  - regions and time zones
    - setting 89
  - registering
    - NetBackup master server or NetBackup EMM server 603
  - Relationship between
    - physical and logical data on a file system 442
  - relocating
    - policy of a tiered file system 490
  - removing
    - a column from a file system 355
    - a column from a tiered file system 480
    - a disk 101
    - disks 98
    - IP address from the cluster 78
    - mirror from a file system 353
    - mirror from a tier spanning a specified disk 481
    - mirror from a tier spanning a specified pool 481
    - mirror from a tiered file system 481
    - policy of a tiered file system 486
    - schedule of a tiered file system 491
    - snapshot schedules 586
    - tier from a file system 495
  - removing a mapping
    - between CIFS and NFS users 203
  - renaming
    - storage pools 105
  - replacing
    - coordinator disks 111
  - replicating file systems
    - setting up 541
  - replication configuration
    - for bandwidth management 538
  - replication destination file system behavior
    - about 568
  - replication destinations
    - accessing 568
  - replication job
    - displaying status 565
    - enabling compression 565
    - managing 557
    - show job 565
  - replication jobs
    - maximum number of parallel 557
  - replication unit
    - setting up files to exclude 546
  - resetting
    - default passwords
      - Master, System Administrator, and Storage Administrator users 24
    - DMP I/O policy 318
    - NetBackup master server or NetBackup EMM server 603
    - NFS statistics 147
  - REST server
    - change user password for 273

- REST server *(continued)*
  - start, stop, or display the status of 271
- restarting the OpenStack Manila driver
  - on the OpenStack controller node 278
- restoring
  - a file system from an instant rollback 592
- restricting
  - metadata information to the primary tier only 495
- resynchronizing
  - stale mirrors on file systems 387
- roles
  - about 27
- route entries
  - deleting from routing tables 68
- routing tables
  - of the nodes in the cluster
    - displaying 68
- RPO report
  - creating 569
- running
  - policy of a tiered file system 486
- S**
- S3
  - ACL 232
- S3 APIs
  - supported by Veritas Access 233
- S3 share
  - managing 438
- SAN client
  - back up 609
- scale-out file system
  - creating and scheduling a policy 505
  - move the files 498
- scale-out file systems
  - about 335
  - configuring the cloud as a tier 497
  - data usage in the cloud tier 507
- scale-out fsck
  - about 385
- schedule
  - displaying for tiered file systems 491
  - modifying for a tiered file system 491
  - removing from a tiered file system 491
- scheduling
  - replication 551
- second tier
  - adding to a file system 478
- security
  - standalone mode 158
- security settings
  - AD domain mode 171
  - changing 161
- server start
  - FTP 241
- server status
  - FTP 241
- server stop
  - FTP 241
- session show
  - FTP 247
- session showdetail
  - FTP 247
- session terminate
  - FTP 247
- set
  - certificate of the REST server 272
- set allow delete
  - FTP 244
- set anonymous login
  - FTP 244
- set anonymous logon
  - FTP 244
- set anonymous write
  - FTP 244
- set home directory path
  - FTP 244
- set listen ipv6
  - FTP 244
- set listen port
  - FTP 244
- set maximum connections per client
  - FTP 244
- set non-secure logins
  - FTP 244
- set security
  - ads for FTP 244
  - FTP 244
- setting
  - AD domain mode 167
  - aio\_fork option 224
  - base distinguished name for the LDAP server 75
  - bind distinguished name for LDAP server 75
  - details of the external mail server 296
  - domain 198
  - domain controller 198
  - domain name for the DNS server 44

- setting *(continued)*
  - domain user name 198
  - events for event reporting 307
  - file system alerts 389
  - filter of the syslog server 301
  - home directory file systems 204
  - IDMAP backend to ad for access to CIFS 184
  - IDMAP backend to hash for accessing CIFS 182
  - IDMAP backend to ldap for trusted domain access to CIFS 180
  - IDMAP backend to rid for access to CIFS 178
  - LDAP password hash algorithm 75
  - LDAP server hostname or IP address 75
  - LDAP server over SSL 75
  - LDAP server port number 75
  - LDAP users, groups, and netgroups base DN 75
  - NIS domain name on all the nodes of cluster 81
  - NTLM 175
  - prior to configuring LDAP 74
  - regions and time zones 89
  - root bind DN for the LDAP server 75
  - severity of the syslog server 301
  - SNMP filter notifications 304
  - SNMP severity notifications 304
  - system date and time 89
  - the NIS server name on all the nodes of cluster 81
  - trusted domains 176
  - trusted domains for the Active Directory 192
  - user quotas for users of specified groups 367
- setting domain user
  - AD domain mode 167
- setting relocation policies
  - best practices 489
- setting security
  - AD domain mode 167
- setting the caching mode 520
- setting up
  - deduplication 445
  - home directories 206
  - replicating file systems 541
- setting up a replication unit
  - to exclude directories and files 546
- severity levels
  - about 296
  - adding to an email group 296
- severity notifications
  - setting 304
- shadow copy
  - making a CIFS share aware 436
- share backend
  - creating on the OpenStack controller node 277
- share directories
  - CIFS and NFS protocols 400
- share properties
  - displaying 431
- shared cache object
  - creating 595
- shares
  - about 398
- show local users
  - FTP 249
- showing
  - snapshot schedules 586
- SmartIO
  - about 509
- snapshot schedules
  - about 582
  - creating 583
  - deleting 586
  - displaying 585
  - modifying 585
  - preserving 586
  - removing 586
  - showing 586
- snapshots
  - about 574
  - creating 575
  - destroying 578
  - displaying 576
  - displaying quotas 578
  - enabling or disabling quota limits 578
  - mounting 580
  - that can be exported
    - displayed 405
  - unmounting 580
- SNMP
  - filter notifications
    - setting 304
  - management server
    - adding 304
    - deleting configured 304
    - displaying current list of 304
  - MIB file
    - exporting to a given URL 304
  - notifications
    - displaying the values of 304

- SNMP *(continued)*
    - server
      - setting severity notifications 304
  - solid-state drives (SSDs)
    - about 509
  - source and destination clusters
    - communicating 528
  - specific workload
    - creating a tuned file system 344
  - specified group
    - deleting a severity from 296
  - specifying
    - DNS name servers 44
  - SSL
    - S3 client 235
    - setting the LDAP server for 75
  - SSL status of the REST server
    - enable or disable 272
  - standalone mode
    - CIFS server status 158
    - CIFS service 158
    - security 158
  - start, stop, or display
    - status of the OpenStack Manila service 273
    - status of the REST server 271
  - starting
    - backup services 604
    - CIFS server 198
    - NFS server 146
    - Veritas Access Replication 524
  - starting CIFS server
    - AD domain mode 167
  - statistics
    - data usage in the cloud tier 507
  - stopping
    - backup services 604
    - NFS server 146
  - storage pools
    - configuring and managing for the OpenStack Manila user 275
    - creating 105
    - destroying 105
    - listing 105
    - listing free space 105
    - moving disks from one to another 98
    - renaming 105
  - storage provisioning and management
    - about 93
  - storing
    - account information 193
    - user and group accounts in LDAP 195
    - user and group accounts locally 195
  - striped file systems
    - creating 346
  - striped tier
    - adding to a file system 478
  - striped-mirror file systems
    - creating 346
  - striped-mirror tier
    - adding to a file system 478
  - striping file systems
    - about 340
  - supported
    - S3 APIs 233
  - swapping
    - network interfaces 63
  - switching
    - CIFS clustering modes from normal to ctdb 212
    - ctdb clustering mode 212
    - from ctdb to normal clustering mode 215
  - syslog format
    - exporting events to a given URL 309
  - syslog server
    - adding 301
    - deleting 301
    - displaying the list of 301
    - displaying the values of 301
    - setting the filter of 301
    - setting the severity of 301
  - system date and time
    - displaying 89
    - setting 89
  - system files
    - hiding when adding a CIFS normal share 429
  - system statistics
    - displaying 310
- ## T
- tier
    - adding a tier to a file system 481
    - displaying location of a specified file 484
    - listing all of the specified files on 483
    - removing a mirror from 481
    - removing a mirror spanning a specified pool 481
    - removing from a file system 495
    - removing from a tier spanning a specified disk 481

- trusted domains
  - allowing access to CIFS when setting an IDMAP backend to ad 184
  - allowing access to CIFS when setting an IDMAP backend to hash 182
  - allowing access to CIFS when setting an IDMAP backend to ldap 180
  - allowing access to CIFS when setting an IDMAP backend to rid 178
  - specifying which are allowed access to the CIFS server 177
- tunables for iSCSI
  - modifying 132
- tuned file system
  - creating for a specific workload 344
- U**
- unexporting
  - share of exported directory 417
- uninstalling
  - NetBackup client 610
- UNIX users from LDAP to Windows users
  - automatic mapping of 204
- unmounting snapshots 580
- Unpinning files from the cache 514
- unplanned failback
  - process overview 573
- unplanned failover
  - process overview 573
- upgrading
  - disk layout versions 394
- use-cases
  - deduplication 442
- user and group accounts in LDAP
  - storing 195
- user and group accounts locally
  - storing 195
- user names
  - mapping for CIFS/NFS sharing 200
- user roles and privileges
  - about 27
- users
  - adding 24
  - adding new 27
  - changing passwords 24
  - deleting 24
- using
  - AD interface 174
  - history command 28
  - using *(continued)*
    - more command 29
    - multi-domain controller support in CIFS 170
    - the Veritas Access CLI 23
- V**
- verifying
  - Veritas Access has joined Active Directory (AD) 166
- Veritas Access
  - about 18
  - configuring to work with OpenStack Manila 269
  - integration with OpenStack Manila 266
  - key features 18
  - logging on to 23
  - product documentation 615
- Veritas Access CLI
  - using 23
- Veritas Access deduplication feature
  - best practices for using 444
- Veritas Access file systems
  - read caching 510
  - writeback caching 512
- Veritas Access file-level replication
  - about 522
- Veritas Access Replication
  - compression 565
  - description of feature 523
  - scheduling 551
  - starting 524
- Veritas Access Replication commands
  - accessing 523
- Veritas Access SmartTier
  - about 476
- Veritas Access to the Kerberos realm
  - adding and configuring 152
- Veritas File System (VxFS)
  - configuring read caching 511
  - customizing caching 514
  - write caching 513
- viewing
  - list of locally saved configuration files 315
  - viewing detailed cache statistics 518
  - viewing file system cache statistics 518
- virtual IP address
  - configuring or changing for NetBackup 606
- virtual name
  - configuring for NetBackup 607

## VLAN

- adding interfaces 57
- configuring interfaces 57
- deleting interfaces 57
- displaying interfaces 57
- volpagemod\_max\_memsz parameter of vxtune
  - modifying 325
- vxtune parameters
  - displaying 325

## W

- what to replicate
  - defining 553
- Windows Active Directory
  - configuring as an IDMAP backend 185
- Workflow
  - object access service 230
- write caching 513
- writeback caching 512
- writeback caching mode 520
- WWN information
  - displaying 102