

Data ONTAP[®] 7.1.0.1

Release Notes

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP

Documentation comments: doccomments@netapp.com

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

Part number 215-01883_A0

21 March 2006

Legal Information

Copyright

Trademarks

Communication regulations information

Compliance

Cables

Canada notice

Avis Canadien

BZT Hinweis

Safety warnings

Contact information

Copyright

Copyright © 1994 – 2006 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

Portions © 1998 – 2001 The OpenSSL Project. All rights reserved.

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

Portions of this product are derived from the Berkeley Net2 release and the 4.4-Lite-2 release, which are copyrighted and publicly distributed by The Regents of the University of California.

Copyright © 1980 – 1995 The Regents of the University of California. All rights reserved.

Portions of this product are derived from NetBSD, which is copyrighted by Carnegie Mellon University.

Copyright © 1994, 1995 Carnegie Mellon University. All rights reserved. Author Chris G. Demetriou.

Permission to use, copy, modify, and distribute this software and its documentation is hereby granted, provided that both the copyright notice and its permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS "AS IS" CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Software derived from copyrighted material of The Regents of the University of California and Carnegie Mellon University is subject to the following license and disclaimer:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain the above copyright notices, this list of conditions, and the following disclaimer.

Redistributions in binary form must reproduce the above copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

All advertising materials mentioning features or use of this software must display the following acknowledgment:

This product includes software developed by the University of California, Berkeley and its contributors.

Neither the name of the University nor the names of its contributors may be used to endorse or promote

products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Portions of the software were created by Netscape Communications Corp.

The contents of those portions are subject to the Netscape Public License Version 1.0 (the "License"); you may not use those portions except in compliance with the License. You may obtain a copy of the License at <http://www.mozilla.org/NPL/>.

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corp. Portions created by Netscape are Copyright © 1998 Netscape Communications Corp. All rights reserved.

This software contains materials from third parties licensed to Network Appliance Inc. which is sublicensed, and not sold, and title to such material is not passed to the end user. All rights reserved by the licensors. You shall not sublicense or permit timesharing, rental, facility management or service bureau usage of the Software.

Portions developed by the Apache Software Foundation (<http://www.apache.org/>). Copyright © 1999 The Apache Software Foundation.

Portions Copyright © 1995 – 1998, Jean-loup Gailly and Mark Adler

Portions Copyright © 2001, Sitrika Inc.

Portions Copyright © 2001, iAnywhere Solutions

Portions Copyright © 2001, i-net software GmbH

Portions Copyright © 1995 University of Southern California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of Southern California, Information Sciences Institute. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

Portions of this product are derived from version 2.4.11 of the libxml2 library, which is copyrighted by the World Wide Web Consortium.

Network Appliance modified the libxml2 software on December 6, 2001, to enable it to compile cleanly on Windows, Solaris, and Linux. The changes have been sent to the maintainers of libxml2. The unmodified libxml2 software can be downloaded from <http://www.xmlsoft.org/>.

Copyright © 1994 – 2002 World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>.

Software derived from copyrighted material of the World Wide Web Consortium is subject to the following license and disclaimer:

Permission to use, copy, modify, and distribute this software and its documentation, with or without modification, for any purpose and without fee or royalty is hereby granted, provided that you include the following on ALL copies of the software and documentation or portions thereof, including modifications, that you make:

The full text of this NOTICE in a location viewable to users of the redistributed or derivative work.

Any pre-existing intellectual property disclaimers, notices, or terms and conditions. If none exist, a short notice of the following form (hypertext is preferred, text is permitted) should be used within the body of any redistributed or derivative code: "Copyright © [Date-of-software] World Wide Web Consortium, (Massachusetts Institute of Technology, Institut National de Recherche en Informatique et en Automatique, Keio University). All Rights Reserved. <http://www.w3.org/Consortium/Legal/>"

Notice of any changes or modifications to the W3C files, including the date changes were made. (We recommend you provide URLs to the location from which the code is derived.)

THIS SOFTWARE AND DOCUMENTATION IS PROVIDED "AS IS," AND COPYRIGHT HOLDERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR THAT THE USE OF THE SOFTWARE OR DOCUMENTATION WILL NOT INFRINGE ANY THIRD PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS.

COPYRIGHT HOLDERS WILL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY USE OF THE SOFTWARE OR DOCUMENTATION.

The name and trademarks of copyright holders may NOT be used in advertising or publicity pertaining to the software without specific, written prior permission. Title to copyright in this software and any associated documentation will at all times remain with copyright holders.

Software derived from copyrighted material of Network Appliance, Inc. is subject to the following license and disclaimer:

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

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

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

Trademarks

NetApp, the Network Appliance logo, the bolt design, NetApp the Network Appliance Company, DataFabric, Data ONTAP, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks of Network Appliance, Inc. in the United States, and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The Evolution of Storage are trademarks of Network Appliance, Inc. in the United States and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, ComplianceClock, ComplianceJournal, ContentDirector, ContentFabric, EdgeFiler, FlexClone, FlexVol, FPolicy, HyperSAN, InfoFabric, LockVault, Manage ONTAP, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapMigrator, SnapSuite, SnapValidator, SohoFiler, vFiler, VFM, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS, SpinHA, SpinMove, and SpinServer are registered trademarks of Spinnaker Networks, LLC in the United States and/or other countries. SpinAV, SpinManager, SpinMirror, SpinRestore, SpinShot, and SpinStor are trademarks of Spinnaker Networks, LLC in the United States and/or other countries.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States

and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

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

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Communication regulations information

Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the users will be required to correct the interference at their own expense.

Cables

To maintain compliance with applicable emission standards, use cables shielded with metallic RFI/EMI connector hoods on this device.

Canada notice

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the radio interference regulations of the Canadian Department of Communications.

Avis Canadien

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le ministère des Communications du Canada.

BZT Hinweis

Hiermit wird bescheinigt, daß dieses Gerät in Übereinstimmung mit den Bestimmungen der BAPT–AmtsblVfg 243/1991 funktentstört ist. Der vorschriftsmäßige Betrieb mancher Geräte (z.B. Meßsender) kann allerdings gewissen Einschränkungen unterliegen. Beachten Sie deshalb die Hinweise in der Bedienungsanleitung.

Dem Bundesamt für Zulassungen in der Telekommunikation wurde das Inverkehrbringen dieses Gerätes angezeigt und die Berechtigung zur Überprüfung der Serie auf die Einhaltung der Bestimmungen eingeräumt.

Safety warnings

You must follow these safety rules when working with this equipment.

WARNING: Failure to follow the directions contained in the following statements could result in bodily harm or loss of life:

- When installing disk shelves and a filer/NetCache appliance into a movable cabinet or rack, install the equipment from the bottom up for best stability.
- DC-based systems must be installed in a restricted access location.
- To reduce the risk of personal injury from hot surfaces, allow the internal components time to cool before touching or installing options.
- To reduce the risk of personal injury or damage to the equipment, ensure that the equipment is properly supported or braced when installing options.

- This equipment is designed for connection to a grounded outlet. The grounding type plug is an important safety feature. To avoid the risk of electrical shock or damage to the equipment, do not disable this feature.
- This equipment is furnished with one or more replaceable batteries. There is danger of explosion if the battery is incorrectly replaced. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

WARNING for units with two power supplies: If your filer, NetCache Appliance, or disk shelf has two power supplies and you need to turn the unit off, heed the following warning:

WARNING: This unit has more than one power supply cord. To reduce the risk of electrical shock, disconnect all power supply cords before servicing.

AVERTISSEMENT: Cet appareil comporte plus d'un cordon d'alimentation. Afin de prévenir les chocs électriques, débrancher tous les cordons d'alimentation avant d'effectuer le dépannage.

ACHTUNG: Dieses Gerät besitzt zwei Netzanschlussleitungen. Vor Wartung alle Anschlüsse vom Netz trennen.

Contact information

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP

Documentation comment: doccomments@netapp.com

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

Table of Contents

Data ONTAP® 7.1.0.1 Release Notes.....	1
About the Data ONTAP® 7.1.0.1 release	1
About these release notes	1
Fixed bugs in Data ONTAP 7.1.0.1	1
Upgrade information	1
Changes introduced in Data ONTAP 7.1.0.1.....	3
New and changed features in the Data ONTAP 7.1 release family.....	4
Manageability enhancements	4
Password aging and improved password security.....	4
Dynamic DNS (DDNS).....	4
Slave NIS.....	4
SNMP updates.....	4
Protocol related enhancements	4
Blocks protocols.....	4
LDAP.....	5
Data protection enhancements	5
LockVault.....	6
Resynchronizing vFiler unit systems after disaster recovery.....	6
VERITAS NetBackup & SnapVault.....	6
Storage resource management enhancements	6
Maintenance Center and disk health management.....	6
Performance improvements for Microsoft Exchange environments.....	6
Policy-based space management.....	6
Windows-related improvements	6
Improved GPO support.....	6
Native file blocking.....	7
Clustering.....	7
Negotiated failover for network interface failures.....	7
Licensing changes	7
New and changed commands and options in the Data ONTAP 7.1 release family.....	8
New commands in Data ONTAP 7.1	8
Changed commands in Data ONTAP 7.1	10
Replaced or removed commands in Data ONTAP 7.1	11
New configuration files in Data ONTAP 7.1	12
New options in Data ONTAP 7.1	12
Replaced or Removed options in Data ONTAP 7.1	15
Requirements for running Data ONTAP 7.1.0.1.....	17
Supported systems	17
Systems you can use in clusters	17
Maximum total capacity supported	17
Storage system firmware	17
Disk firmware	17
Important cautions.....	18
If you are replacing traditional volumes with FlexVol volumes	18
If you see unexpected warnings and messages regarding FlexVol volumes	18
If you are updating disk firmware or you are upgrading Data ONTAP software in systems with DS14 or DS14Mk2 shelves (such as FAS250 or FAS270 systems)	19
Special considerations for clustered storage systems.....	19
Checking disk firmware versions.....	19
If you upgrade storage systems that contain two or more non-original disk drives	19
About software-based disk ownership.....	20

Table of Contents

Important cautions

How disk ownership can be enabled.....	20
Preventing and correcting accidental enabling of software-based disk ownership.....	20
How data could be lost when disk ownership is inadvertently enabled.....	21
If you upgrade storage systems with iSCSI targets	21
If you upgrade from releases earlier than Data ONTAP 6.5	21
If you upgrade from Data ONTAP 6.4.x and use CHAP authentication with iSCSI	22
If you upgrade systems running SnapMirror	23
If you are running DataFabric Manager with a Business Continuity License enabled	23
If you have a SnapLock Compliance license	23

Known Problems and Limitations.....25

Manageability issues.....	25
4 Gb HBA is not recognized by earlier diagnostics software.....	25
Synchronous SnapMirror and FlexVol volumes.....	26
SSH Secure Shell/SSH Tectia client does not work properly unless forwarding is disabled	26
Maximum number of SSH sessions	26
Long-running commands invoked using SSH may be terminated	26
SSH authentication agent forwarding is not supported	26
Pseudo-terminals are not supported for SSH	26
PuTTY command line editing does not work properly	26
Non-local users cannot use login protocols	26
FilerView does not support roles and capabilities for all tasks.....	26
No secondary image on systems with 32 MB CompactFlash cards	27
Reversion cannot take place during inode-to-pathname initialization	27
Protocol issues	27
NFSv4 client compatibility	27
NFS configuration issue for Hummingbird with Kerberos	28
Client notification messages in Windows domains require NetBIOS	28
Unsupported Windows features in the file serving environment.....	28
Do not use vlan delete -q with IPsec	28
iSNS service and Microsoft iSNS Server v.3.0	28
Enable caching with NIS lookup	29
Group Policy Objects (GPOs) are applied differently on storage systems and Windows systems	29
Data protection issues	29
Stagger Snapshot copy schedules to avoid transfer conflicts	29
Synchronous SnapMirror and storage system performance	29
vscan feature does not support NIS authentication	29
Compatibility with SnapDrive and Snap Manager	30
FlexVol volumes cannot be migrated using SnapMover	30
Potentially reduced performance for IPsec traffic	30
Storage resource management issues.....	30
Default quota requirement	30
Changing the IP address of a FlexCache origin storage system	30
Partition alignment problems cause an iSCSI LUN performance problem	30
CFO partner node's SSL certificate is used after takeover and giveback	30
LUNs in FlexCache volumes	30
Qtree path not shown in quota report for new qtrees.....	31
Change in sysstat -x command output.....	31

Changes to published documentation.....32

Changes to the System Configuration Guide.....	32
Changes to the Storage Management Guide.....	32
Displaying disk space usage on an aggregate.....	32
Change to the Block Access Management Guide for iSCSI and FCP.....	32
Changing the adapter speed.....	32

Table of Contents

Changes to published documentation	
Example.....	33
Where to find product documentation and other information.....	35
Documentation Roadmap	35
Finding documentation on NOW	35
Searching online information	35

Data ONTAP® 7.1.0.1 Release Notes

About the Data ONTAP® 7.1.0.1 release

Data ONTAP® 7.1.0.1 is a General Availability (GA) release in the Data ONTAP 7.1 release family.

Note

This release supports only FAS3000 series systems with 4 Gb Fibre Channel target Host Bus Adapters (HBAs) and should not be installed or run on any other NetApp® storage systems. For more information, see "Requirements for running Data ONTAP 7.1.0.1."

For more information on the Data ONTAP release model, including a definition of a GA release, see the Data ONTAP Release Model.

About these release notes

Note

These release notes are designed primarily to be used online. A PDF is available for those who need a printer-friendly copy of the text.

The information in this document applies only to the Data ONTAP 7.1.0.1 release for the NetApp FAS3000 series storage systems with 4 Gb target HBAs.

Note

The terms "flexible volumes" and "FlexVol™ volumes" are used interchangeably in Data ONTAP documentation.

Fixed bugs in Data ONTAP 7.1.0.1

To request a list of the bugs fixed since your current version of Data ONTAP was released, see the Data ONTAP – Release Comparison page .

To request more information about an individual bug and to explore other bug-related tools, see Bugs Online .

Upgrade information

If you are upgrading to this release, make sure that you also read both of the following:

- Important cautions. ***You must read these before downloading Data ONTAP.***

This information helps you identify and resolve issues that might affect the availability of your systems. Check this online version of the *Release Notes* periodically for new cautions or updates that may have been posted since you downloaded your software.

- The *Upgrade Guide*.

This guide describes how to upgrade to the Data ONTAP 7.1 release family and provides information you need before upgrading your software or reverting it to an earlier version. This information is particularly important if you are upgrading from a release earlier than Data ONTAP 6.5.

Data ONTAP 7.1.0.1 Release Notes

Legal Information

Last updated: 21-Mar-2006 15:10

Changes introduced in Data ONTAP 7.1.0.1

Note

If this is the first release you are installing in the Data ONTAP® 7.1 release family, it is not necessary to read this section. You can go directly to "New and changed features in the Data ONTAP 7.1 release family."

Data ONTAP 7.1.0.1 adds support for the QLogic QLA2462 PCI-x 4 Gb Fibre Channel target Host Bus Adapter (HBA) on FAS3000 series storage systems. For more information, see "4 Gb target HBA support" and "Requirements for running Data ONTAP 7.1.0.1."

A new option has been added to the **fcv config** command to configure the speed of the new 4 Gb target HBA. For more information, see "Changed commands in Data ONTAP 7.1."

Two new known limitations have been identified in Data ONTAP 7.1.0.1:

- "4 Gb HBA is not recognized by earlier diagnostics software"
- "Change in sysstat -x command output"

Legal Information

Last updated: 21-Mar-2006 17:06

New and changed features in the Data ONTAP 7.1 release family

This section covers features that were added or changed in the Data ONTAP® 7.1 release family. The topics below describe the major changes; see also New and changed commands and options.

- Manageability enhancements
- Protocol related enhancements
- Data protection enhancements
- Storage resource management enhancements
- Windows-related improvements
- Clustering
- Licensing changes

Manageability enhancements

Password aging and improved password security

Provides support for site-determined password aging policies and support for RFC 2307.

Dynamic DNS (DDNS)

Dynamic updates to the Domain Name System (DNS) allow the storage system to automatically update DNS servers with its DNS information. DNS updates have to be enabled on the storage system as well as the DNS server.

Slave NIS

You can now configure a storage system to maintain a slave copy of the Network Information System (NIS) maps. Unless the NIS maps are very large and are updated frequently, using a slave NIS database improves performance and reduces network traffic.

SNMP updates

Data ONTAP 7.1 includes a new Simple Network Management Protocol (SNMP) trap in the NetApp custom Management Information Base (MIB) file. The new maxdirsize trap causes an alert to be sent when the 64MB directory limit is nearly reached or has been reached.

Protocol related enhancements

Blocks protocols

Blocks protocol enhancements include the following:

- Improved support for iSCSI
 - ◆ Support for multiple iSCSI connections per session

Multiple iSCSI connections per session improves high availability and bandwidth aggregation. The multiple iSCSI connection feature provides sophisticated error recovery techniques that reduce the impact of error conditions on applications.

- ◆ Support for iSCSI error recovery levels 1 and 2

Improves data transmission error handling and recovery with initiators that also support this feature.

- Single_image FCP port mode

Single_image FCP port mode is a new cfmode. With single_image mode, all LUNs in the cluster are exported on all FCP target ports in the cluster. The cluster has a single global FCP nodename. Any request that storage system A receives that cannot be mapped to a LUN mapped on storage system A is sent across the interconnect to storage system B. LUN maps are checked across both storage systems for conflicts.

- Port sets

Port sets can be used when FCP single_image mode is on, and with non-clustered systems, to provide the ability to define sets of target and initiator ports. By binding an igroup to a port set, you can control which LUNs can be seen by which ports.

- 4 Gb target HBA support

Data ONTAP 7.1.0.1 and higher supports the QLogic QLA2462 PCI-x 4 Gb Fibre Channel target Host Bus Adapter (HBA) on the FAS3000 series storage systems. For more information, see "Change to the Block Access Management Guide for iSCSI and FCP".

Note: Only single_image and standby cfmodes are supported with this HBA. If you upgrade from a prior version of Data ONTAP and want to use the 4Gb HBA, you must manually change the cfmode to single_image. For more information, see *Changing the Cluster cfmode Setting in Fibre Channel SAN Configurations*.

For more information about blocks protocols, see the *Block Access Management Guide for iSCSI and FCP*.

For more information about CIFS, FTP, HTTP, LDAP, and NFS protocol support, see the *File Access and Protocols Management Guide*.

LDAP

LDAP (Lightweight Directory Access Protocol) enhancements are summarized here (for more information see the *File Access and Protocols Managements Guide*):

- LDAP over SSL

LDAP (Lightweight Directory Access Protocol) over SSL (Secure Sockets Layer) adds the ability to encrypt and authenticate LDAP traffic using cryptographic certificates over SSL. (SSL support already exists on Data ONTAP, but previously LDAP could not use it.) Secure LDAP is supported against all LDAP servers, including OpenLDAP and Windows Active Directory. Mutual (client side) authentication is not currently supported.

- LDAP authentication using Simple Authentication and Security Layer (SASL)

The Simple Authentication and Security Layer (SASL) is a method for adding authentication support to connection-based protocols. By using SASL, a user can be authenticated to an LDAP server without passing the user password in clear text. SASL requires a mechanism to be negotiated between the client and the server before doing the user authentication. There are several industry standard authentication mechanisms that can be used with SASL, including GSSAPI for Kerberos V, DIGEST-MD5, and Plain and External for use with Transport Layer Security (TLS).

Data protection enhancements

LockVault

LockVault enhances existing SnapLock functionality and builds SnapVault features on top of basic and enhanced SnapLock functionality. LockVault provides a solution for sites where data must be retained for specific periods of time. For example, LockVault allows for compliance with various regulations, such as SEC 17a-4 and Sarbanes-Oxley.

Resynchronizing vFiler unit systems after disaster recovery

The **vfiler unit dr resync** command enables you to resynchronize your original vFiler unit with the currently activated disaster-recovery vFiler unit before bringing up the original vFiler unit.

VERITAS NetBackup & SnapVault

Data ONTAP 7.1 includes two new integration points with VERITAS NetBackup software. First, NBU can now be used to configure & manage SnapVault relationships. Second, SnapVault on Nearstore now provides a space-efficient backup target for NBU-managed backups on non-NetApp primary storage.

Storage resource management enhancements

Maintenance Center and disk health management

Maintenance Center adds an improved disk health assessment test, and, if a drive does not meet the requirements of health assessment, Maintenance Center determines if the disk can still be used as a spare or if it needs to be returned to NetApp.

For more information, see the *Storage Management Guide*.

Performance improvements for Microsoft Exchange environments

WAFL extents are a performance improvement feature for Microsoft Exchange environments. WAFL extents are off by default and controlled through the **vol** command **options vol-name extent**.

Policy-based space management

Policy-based space management provides a variety of space reservation settings including thin provisioning or underprovisioning and fractional reservations. Policy-based space management helps a storage administrator keep the amount of unutilized space on a storage system to a minimum. Policy-based space management includes these functions:

- Snapshot autodelete
- Volume autosize

Windows-related improvements

Improved GPO support

Data ONTAP 7.1 includes improved support for Windows Group Policy Objects (GPOs), which enable policy-based administration for computers in an Active Directory environment. Supported GPOs include a File System security policy, an Event Log, Auditing, and startup and shutdown scripts. For details, see the *File Access and Protocols Management Guide*.

Native file blocking

Data ONTAP 7.1 provides new file screening software that runs natively on the storage system, in addition to existing support for third-party file screening software that runs on client systems. Native file blocking provides simple denial of restricted file types. For more information, see the *File Access and Protocol Management Guide*.

Clustering

Negotiated failover for network interface failures

Negotiated failover provides a framework that allows nodes in a cluster to exchange health status information using up to four NIC interfaces. If one node is healthy and its partner is not, the healthy node takes over. If both nodes become impaired, no takeover is triggered.

Licensing changes

There are no licensing changes.

Legal Information

Last updated: 21-Mar-2006 13:26

New and changed commands and options in the Data ONTAP 7.1 release family

This section provides information about the commands, options, and configuration files that have been changed or added to the Data ONTAP® 7.1 release family. These changes are described in the following topics:

- New commands in Data ONTAP 7.1
- Changed commands in Data ONTAP 7.1
- Replaced or removed commands in Data ONTAP 7.1
- New configuration files in Data ONTAP 7.1
- New options in Data ONTAP 7.1
- Replaced or removed options of Data ONTAP 7.1

New commands in Data ONTAP 7.1

For each command family and each command, the following table gives this information:

- The purpose of the command
- The location of documentation about the feature

Command	Purpose	Documentation
cifs gpresult	Displays information about the Windows Group Policy Objects (GPOs) currently applicable to the storage system and the results of applying them	na_cifs(1) man page <i>File Access and Protocols Managements Guide</i>
cifs gpupdate	Updates GPOs on the storage system with the most current Group Policy settings available in an Active Directory domain	na_cifs(1) man page <i>File Access and Protocols Managements Guide</i>
disk checksum {<i>disk_name</i> all} [-c block zoned]	Specifies the checksum type (block or zone) for one or all ATA drives. The default is block checksums	na_disk(1) man page
iscsi alias	Creates a new iSCSI alias	na_iscsi(1) man page

Data ONTAP 7.1.0.1 Release Notes

iscsi portal	Displays a list of the portals (IP address and/or TCP port number), and their portal group assignments, over which the storage system operates the iSCSI service	na_iscsi(1) man page
iscsi tpgroup	Manages the assignment of storage system network interfaces to target portal groups	na_iscsi(1) man page
keymgr	Manages security certificates	na_keymgr(1) man page
portset help	Lists portset commands	na_portset(1) man page
portset add	Adds a port to a portset	na_portset(1) man page
portset create	Creates a new portset	na_portset(1) man page
portset destroy	Destroys portsets	na_portset(1) man page
portset remove	Removes ports from a portset	na_portset(1) man page
portset show	Displays portsets	na_portset(1) man page
snap autodelete	Automatically deletes Snapshots when the flexible volume is nearly full	na_snap(1) man page
storage show disk -x	Displays disk-specific information including serial number, vendor name, and model	na_storage(1) man page
vol autosize	Configures a FlexVol volume to grow automatically when it is nearly full	na_vol(1) man page <i>Storage Management Guide</i>
vol create trad_volname [-L [compliance	Specifies type of SnapLock volume being created. Only needed if both SnapLock Compliance and SnapLock Enterprise are licensed	na_vol(1) man page <i>Data Protection Online Backup and Recovery Guide</i>

enterprise]]		
vol options <i>vol-name</i> no_i2p [on off]	Disables the inode to pathname scanner	na_vol(1) man page
vol options <i>vol-name</i> extent	Enables application writes to be written in the volume as a write of a larger group of related data blocks called an extent	na_vol(1) man page
vol options <i>vol-name</i> try_first [volume_grow snap_delete]	Defines how Data ONTAP reclaims space when a volume is nearly full specifically, whether to automatically increase the volume first or whether to automatically delete Snapshot copies first	na_vol(1) man page

Changed commands in Data ONTAP 7.1

For each command, the following table gives this information:

- The change in the command
- The location of documentation about the feature

Command	Change	Documentation	Release Introduced
fcg config	Now includes the speed option, which allows you to change the speed setting for an adapter (in Gb/second). Depending on the capability of your adapter, you can set the speed to 4, 2, 1, or auto (auto-negotiation, which is the default).	na_fcg(1) man page "Change to the Block Access Management Guide for iSCSI and FCG"	7.1.0.1
ifconfig		na_ifconfig(1) man page	7.1

	Now includes the -nfo option which specifies that negotiated failover is to be disabled for the network interface. This option applies only to storage systems in a cluster.	<i>Network Management Guide</i>	
iscsi stats	Now reports statistics for the entire storage system, instead of for an individual adapter	na_iscsi(1) man page	7.1
useradmin	Now includes the options -m and -M . The -m option specifies the minimum allowable age of the user's password (in days) before the user can change it again. The -M option specifies the maximum allowable age of the user's password (in days).	na_useradmin(1) man page <i>System Administration Guide</i>	7.1
vol options volname [optname optval]	Now adds the maximum retention period infinite for the options snaplock_maximum_period , snaplock_default_period , and snaplock_minimum_period fconfig	na_vol(1) man page	7.1

Replaced or removed commands in Data ONTAP 7.1

The following commands are deprecated or removed:

- **dafs**, removed
- **iswt interface**, replaced by **iscsi interface**
- **iswt session show**, replaced by **iscsi session show**

- **iswt connection show**, replaced by **iscsi connection show**
- **iscsi show initiator**, replaced by **iscsi initiator show**
- **iscsi config**, removed
- **iscsi show adapter**, removed

New configuration files in Data ONTAP 7.1

There are no new configuration files in Data ONTAP 7.1

New options in Data ONTAP 7.1

For each new option that can be used with the **options** command, the following table gives this information:

- A description of the option's purpose
- The allowed values, or the type of the value, or an example value used with the option

For more information about the **options** command and individual options, see the `na_options(1)` man page.

Option	Purpose	Default value or example
cf.takeover.on_network_interface_failure	Allows negotiated takeover to be enabled when the cluster nodes detect failures in network interfaces. Only those network interfaces that have explicitly enabled negotiated failover via the ifconfig command will be monitored.	off (on off)
cf.takeover.on_network_interface_failure.policy	Determines what policy to apply for triggering negotiated failover when network interfaces fail	all_nics (all_nics any_nics)
cf.takeover.on_short_uptime	Determines whether a cluster failover will happen if a storage system fails within sixty seconds of booting up	on (on off)
cifs.audit.nfs.enable	Enables CIFS auditing of files in UNIX security style qtrees. When enabled, auditable events	off (on off)

Data ONTAP 7.1.0.1 Release Notes

	performed on these files are recorded in the log file. Auditable events are specified by the Windows System Access Control Lists (SACLs) either on the file itself, or on the file specified in the value of <code>cifs.audit.nfs.filter.filename</code>	
<code>cifs.audit.nfs.filter.filename</code>	Points to the filter file used to identify which file events get included in the CIFS log by default. When an operation is performed on UNIX security style qtree files that have no SACL set, the SACL set on the file identified by this option is used to determine which events get logged.	none
<code>cifs.client.dup-detection</code>	Directs Windows servers to attempt to detect duplicate sessions in order to terminate any sessions that did not terminate when a client system rebooted	name (name ip-address off)
<code>cifs.gpo.enable</code>	Enables/disables GPO support on storage systems	on off (default off)
<code>cifs.gpo.trace.enable</code>	Enables/disables display of GPO diagnostic information	on off (default off)
<code>disk.maint_center.spares_check</code>	Enables/disables checking the number of available spares before Data ONTAP puts a disk that has exceeded the threshold of media errors into the maintenance center	on off (default on)
<code>iscsi.isns.rev</code>	Determines the draft level of the iSNS specification the iSNS service on the storage system is compatible with	22 (example iSNS specification draft level)
<code>iscsi.max_connections_per_session</code>	Specifies the number of iSCSI connections per session allowed by the storage system	The default is use_system_default , which currently equals 1.

Data ONTAP 7.1.0.1 Release Notes

iscsi.max_error_recovery_level	Specifies the maximum iSCSI error recovery level allowed by the storage system	The default is use_system_default , which currently equals 0.
kerberos.replay_cache.enable	Prevents passive replay attacks by storing user authenticators on the filer, and by insuring that the authenticators are not reused by attackers <i>Note</i> Storing and comparing the user authenticators can result in a substantial performance penalty for higher workloads on the filer.	off (on off)
nfs.notify.carryover	Specifies that when set to off, the hosts present in the /etc/sm/notify file are not sent Network Status Monitor (NSM) reboot notifications after a storage system panic/reboot	on (on off)
nfs.v4.acl.enable	Specifies that when enabled, Access Control Lists (ACLs) are supported for NFS version 4. The ACL option controls setting and getting NFSV4 ACLs. It does not control enforcement of these ACLs for access checking. This feature is not supported over NFS versions 2 and 3.	off (on off)
nis.netgroup.domain_search.enable	Specifies whether netgroup entry comparisons will consider the domain names in the search directive from /etc/resolv.conf	on (on off)
nis.slave.enable	Enables an NIS slave on the storage system	off (on off)
security.passwd.firstlogin.enable	Controls whether all administrators (except for root) must change their passwords upon first login. A value of on means that newly created administrators, or administrators whose passwords were changed by another	off (on off)

Data ONTAP 7.1.0.1 Release Notes

	administrator, may only run the passwd command until they change their password again.	
security.passwd.lockout.numtries	Controls how many attempts an administrator can make to log in before the account is disabled. This account may be reenabled by having a different administrator change the disabled administrator's password. If the new password value is 0, then it remains unused, and failing to log in will never disable an account.	4, 294, 967, 295
security.passwd.rules.history	Controls whether an administrator can reuse a previous password. A value of 5 means that the appliance will store 5 passwords, none of which an administrator can reuse. A value of 0 means that an administrator is not restricted by any previous password. Make sure that the security.passwd.rules.enable command has the value on or security.passwd.rules.history is ignored.	0
snapvault.lockvault_log_volume	Configures the LockVault Log Volume. Valid values for this option are online SnapLock volume names.	sl_vol1

Replaced or Removed options in Data ONTAP 7.1

The following options have been replaced or removed in this release:

- **cifs.restrict_anonymous.enable** (replaced by **cifs.restrict_anonymous**)
- **iscsi.iswt.tcp_window_size** (replaced by **iscsi.tcp_window_size**, although **iscsi.iswt.tcp_window_size** continues to be the command for backwards compatibility)

Data ONTAP 7.1.0.1 Release Notes

Legal Information

Last updated: 21-Mar-2006 17:05

Requirements for running Data ONTAP 7.1.0.1

This section lists the storage systems and firmware you need in order to run Data ONTAP 7.1.0.1 and run clustered systems.

Supported systems

Data ONTAP 7.1.0.1 supports only FAS3000 series systems with 4 Gb Fibre Channel target Host Bus Adapters (HBAs) and should not be installed or run on any other NetApp storage systems.

Note

- If you want to run NetApp diagnostics software on the 4 Gb target HBAs, you must use diagnostics version 4.6.5 or later. Earlier versions of diagnostics software do not recognize 4 Gb target HBAs. Diagnostics version 4.6.5 is available from the Service Image Archive for Diagnostics and Common Firmware Executable (on the NOW site at http://now.netapp.com/NOW/download/tools/serviceimage/archive_fas3000.shtml).
- For information about installing 4 Gb target HBAs in storage system expansion slots, see "Changes to the System Configuration Guide".

Systems you can use in clusters

Only FAS3050c and FAS3020c clustered storage systems are supported in Data ONTAP 7.1.0.1.

FAS3000 series systems support clusters regardless of whether the shelf connected to the system is FC-AL or ATA.

Maximum total capacity supported

For information about your storage system model's capacity and maximum volume size, see the *System Configuration Guide*.

Storage system firmware

It is best to upgrade to the latest version of system firmware for your storage system. For a list of available system firmware, see the System Firmware Release Table.

Note

The latest system firmware is included with Data ONTAP upgrade packages for CompactFlash®-based storage systems. For more information, see the *Upgrade Guide*.

Disk firmware

For information about the latest disk firmware, see the Disk Drive & Firmware Matrix (on the NOW site at <http://now.netapp.com/NOW/download/tools/diskfw/>).

Note

New disk firmware is sometimes included with Data ONTAP upgrade packages. For more information, see the *Upgrade Guide*.

Legal Information

Last updated: 21-Mar-2006 15:25

Important cautions

Before upgrading to this Data ONTAP 7.1 release, make sure that you read the following items to identify and resolve issues that might affect the operation of your storage systems.

- If you are replacing traditional volumes with FlexVol volumes
- If you see unexpected warnings and messages regarding FlexVol volumes
- If you are updating disk firmware or you are upgrading Data ONTAP software in systems with DS14 or DS14Mk2 shelves (such as FAS250 or FAS270 systems)
- If you upgrade storage systems that contain two or more non-original disk drives
- If you upgrade storage systems with iSCSI targets
- If you upgrade from releases earlier than Data ONTAP 6.5
- If you upgrade from Data ONTAP 6.4.x and use CHAP authentication with iSCSI
- If you upgrade systems running SnapMirror
- If you are running DataFabric Manager with Business Continuance License enabled
- If you have a SnapLock Compliance license

If you are replacing traditional volumes with FlexVol volumes

Flexible volumes have different best practices, optimal configurations, and performance characteristics than traditional volumes. Make sure you understand these differences by referring to the FlexVol volume documentation and deploy the configuration that is optimal for your environment.

For information about deploying a storage solution with flexible volumes, including migration and performance considerations, see the technical report *Introduction to Data ONTAP Release 7G* (available from the Data ONTAP 7G Online Community Page on the NOW site). For detailed information about configuring FlexVol volumes and aggregates, see the *Storage Management Guide*.

If you see unexpected warnings and messages regarding FlexVol volumes

If an aggregate is unexpectedly taken offline because of a hardware failure, for example if you have an aggregate on a loop and the loop fails, you might see unexpected warnings and messages. Data ONTAP assigns a unique file system identifier (FSID) to every FlexVol volume on a system. Data ONTAP cannot check the FSIDs of offline flexible volumes. Data ONTAP does detect the possibility of FSID conflict and issues warnings and messages alerting you to the possibility of duplicate FSID creation.

During the time the aggregate is offline you may see warnings and messages during operations such as these:

- Creating a new FlexVol volume, including by cloning

In this case you will see a warning. You can override the warning, but if you do you might see additional problems.

- Bringing a FlexVol volume online

Before the FlexVol volume is brought online, Data ONTAP checks the FSID. If there is a duplicate FSID you see the following message:

```
vol online: FSID marked invalid because it already exists. Unable to bring
volume 'volname' online
```

The volume does not come online. You cannot override this warning. Knowledge Base article kb4361 provides additional information.

- Accessing of a volume by a vFiler unit

You might see a message from the vFiler unit about a volume being in an unexpected state. The volume reported might not be an offline volume. NFS clients will not be able to access the reported vFiler volume. You can fix this problem by first taking the volume offline: `vol offline vol1` and then bringing the volume back online: `vol online vol1`.

If you are updating disk firmware or you are upgrading Data ONTAP software in systems with DS14 or DS14Mk2 shelves (such as FAS250 or FAS270 systems) ▲

Important

If you are currently running a version of Data ONTAP that does not include a fix for Bug ID 113823, do **not** update disk firmware before upgrading to Data ONTAP 7.1, or you could damage disks, resulting in data loss. A list of releases where this bug is fixed is found in Bug ID 113823.

Disk firmware is automatically updated during the Data ONTAP upgrade whenever the disk drives have a firmware version older than the firmware version that is included with the ONTAP release. As disk firmware is updated, it is possible (though unlikely) that all disk drives on a shelf will receive the update at the same time. This simultaneous update might cause the firmware update process to fail, rendering the disks unusable and causing loss of data if the failure occurs to multiple disks in the same RAID group.

This problem is described further in Bug ID 113823. Data ONTAP 7.1 includes a fix for Bug ID 113823 that prevents firmware from being concurrently updated on all disk drives.

Note

Bug 113823 occurs only when **every** disk drive on the shelf requires an update.

Special considerations for clustered storage systems

Important

If you have clustered storage systems running a version of Data ONTAP 6.5x that does not include the fix for Bug ID 113823, do **not** perform a nondisruptive upgrade to any release in the Data ONTAP 7.1 family. A complete list of releases where this bug is fixed is found in Bug ID 113823.

To avoid this problem, **do not download disk firmware before upgrading**. Upgrade using the standard procedure for upgrading firmware on clustered storage systems.

Checking disk firmware versions

If you have AutoSupport enabled, you can use AutoSupport to verify your disk firmware version in advance and find out whether your system is vulnerable to Bug ID 113823. If AutoSupport indicates that all disks on a disk shelf need firmware updates, failure to follow the instructions in this Important Caution could cause disk drive damage and data loss.

For instructions to use AutoSupport to detect outdated disk firmware, see the *Upgrade Guide*.

If you upgrade storage systems that contain two or more non-original disk drives ▲

Under certain conditions, it is possible to inadvertently enable software-based ownership on a storage system that previously used a hardware-based ownership scheme. When this occurs, volumes on disks that have no software-based

ownership information will be unavailable, which may prevent Data ONTAP from starting up. Though unlikely, there is also a slight potential for data to be lost, as described later in this discussion of disk ownership during upgrades.

To learn more about this and to ensure that you do not have problems at startup and do not risk data loss, read and use the following information:

- About software-based disk ownership
- How disk ownership can be enabled
- Preventing and correcting accidental enabling of software-based disk ownership
- How data could be lost when software-based disk ownership is inadvertently enabled

About software-based disk ownership

With versions of Data ONTAP earlier than 6.5.1, most storage systems use hardware-based disk ownership—that is, disk ownership is based on the physical location of the disk drive. (The FAS270 and FAS270c supported software-based disk ownership starting with the release of Data ONTAP 6.5.) Data ONTAP 6.5.1 and later provide the ability for you to designate disk ownership, rather than letting Data ONTAP automatically assign ownership based on the location of the disk drive. This ownership information gets stored on the disk. When Data ONTAP starts, it determines ownership by retrieving any ownership information on the disk. If no software ownership information is present, hardware disk ownership is assigned based on disk location.

Note

When a disk drive is added to a hardware-based ownership system while Data ONTAP is running, Data ONTAP automatically removes all (software-based) disk ownership information from the disk; ownership information can also be removed manually by booting the storage system in maintenance mode and using the `disk remove_ownership` command.

How disk ownership can be enabled

Accidental enabling of software-based disk ownership happens only when all of the following conditions are met:

- A storage system that uses hardware-based disk ownership has two or more disk drives replaced while Data ONTAP is not running. (If the disk drives are replaced while Data ONTAP is running, the software-based ownership information is automatically deleted from the disks.)
- The replacement disk drives came from a FAS270 or FAS270c storage system running Data ONTAP 6.5 or later, or the disk drives came from any storage system running Data ONTAP 6.5.1 or later, on which software-based disk-ownership was enabled.
- The replacement disk drives have not had ownership information removed after they were installed in the software-based ownership environment.
- The storage system attempts to boot using Data ONTAP 6.5.1 or later, without first entering maintenance mode to remove the ownership information from the replacement disk drives.

When all of these conditions are met, the storage system converts to using a software-based ownership scheme. If this happens, only disks with software-based ownership information on them will be available at startup. Data ONTAP may fail to boot, and there is a small possibility that data could be lost.

Preventing and correcting accidental enabling of software-based disk ownership

To avoid accidental conversion to software-based disk ownership, complete the following steps the first time you start the storage system after the upgrade process.

Note

If you have already experienced an accidental conversion to software-based ownership, use this same procedure to start the storage system in maintenance mode and remove ownership information from the replacement disks.

1. Watch the console as you boot the storage system for the first time following the upgrade process.
2. If you see the message "software ownership has been enabled for this system," enter Ctrl-C to display the special boot menu. If you don't see this message, the storage system is still using hardware-based ownership; discontinue this procedure and boot the storage system in normal mode.
3. Choose option 5, "Maintenance mode boot."
4. Use the `disk remove_ownership` command to remove ownership information from the replacement disks.

Note

This problem can also occur after the upgrade, if you replace disk drives while the storage system is not running. This ownership issue does not occur when you add disks to NearStore appliances or to FAS270 or FAS270c storage systems.

How data could be lost when disk ownership is inadvertently enabled

The following sequence of events describes a scenario that creates conditions under which data could be lost or rendered inaccessible during accidental enabling of software-based disk ownership.

1. A storage system is running one of certain versions of Data ONTAP (including Data ONTAP 7.1) with software-based ownership enabled. (Software-based ownership information has been written to the storage system's disks.)
2. The storage system is modified to run Data ONTAP 6.5. Because Data ONTAP 6.5 does not include software-based ownership, the ownership information on the disks is ignored.
3. One or more replacement disks without software-based ownership information are installed, and volumes are created on those disks.
4. The storage system is upgraded back to the original version of Data ONTAP.

Result: Upon startup, disks that don't contain ownership information are not included in the boot; instead, Data ONTAP perceives them to be unowned disks. Data in volumes on those disks is still present but not visible. Any hidden volume data stored in the NVRAM, due to a crash or other incomplete shutdown, is lost.

To restore access to data on volumes that become hidden due to this issue, remove disk ownership information, as described in "Preventing and correcting accidental disk ownership."

If you upgrade storage systems with iSCSI targets

In Data ONTAP 7.1, the iSCSI target portal group tags have changed from the values used in previous releases. You must reconfigure any Linux or HP-UX iSCSI hosts that use these tags or they will not be able to identify the iSCSI target provided by the NetApp storage system. For more information, see the *Upgrade Guide*.

If you upgrade from releases earlier than Data ONTAP 6.5

If you have already upgraded to the Data ONTAP 6.5 release family from an earlier release and are now upgrading from 6.5 to 7.1, the following cautions do not apply to you. See the *Upgrade Guide* for information about upgrade procedures.

If you are planning to upgrade from a release earlier than Data ONTAP 6.5, make sure to read the following cautions:

- For NetApp storage systems that have CompactFlash™ cards and that run Open Firmware, you must upgrade the system firmware and diagnostics files to version 4.2.2 or later before upgrading to Data ONTAP 7.1. Follow these guidelines:
 - ◆ If you are running Data ONTAP 6.4.1 on a storage system that has a CompactFlash card and that is running Open Firmware, you must complete an additional procedure **before** upgrading firmware to 4.2.2.
For more information, see Bug ID 98952.

Data ONTAP 7.1.0.1 Release Notes

- ◆ If you downloaded and installed the 4.2.2 or the 4.2.3 system firmware upgrade, you must run the `set-defaults` command from the firmware OK prompt before rebooting.
For more information, see Bug ID 105365.
- ◆ If you are upgrading from 4.2.2 or 4.2.3 to 4.3 or later system firmware, you must run the `set-defaults` command from the firmware OK prompt before rebooting into the new firmware version.
- ◆ If you are running 4.3 or later system firmware, do not run the `set-defaults` command.
- If you are running a version of Data ONTAP earlier than 6.4.2 on a system that has a CompactFlash card and that is running Open Firmware, you must upgrade to the latest Data ONTAP 6.4.x release before upgrading to Data ONTAP 7.1.
- If you are running Data ONTAP 6.3.2 or earlier on a diskette-based system, you must upgrade to the latest Data ONTAP 6.3.x release before upgrading to Data ONTAP 7.1.
- If you are upgrading to Data ONTAP 7.1, configure your Fibre Channel–Arbitrated Loop (FC–AL) adapters before 1–Gb and 2–Gb operations.
For more information, see the flyer "Configuring new and existing FC–AL adapters" in the Hardware Information Library.
- To prepare for the upgrade, use the following procedure:
 - ◆ Upgrade during nonpeak hours.
 - ◆ Keep the storage system workload moderate to enable a faster upgrade.
 - ◆ If you are serving files with CIFS, make sure that the file system is not 100 percent full.

Note

Upgrading to the Data ONTAP 7.1 release family can take significantly longer to complete than upgrades to earlier releases. Depending on your system and how it is configured, the 7.1 upgrade can take several hours. However, the 7.1 upgrade takes place in the background, so the system is completely available during the upgrade.

- The upgrade to Data ONTAP 7.1 must be complete before you can revert to a previous version.
- If you are upgrading to Data ONTAP 7.1 in a Storage Area Network (SAN) with Solaris Fibre Channel hosts and you are using the NetApp-supplied Array Support Library (ASL) 1.0, you must upgrade to the ASL 2.0 before upgrading to the Data ONTAP 7.1 release family.
For more information, see the *SAN Host 1.3 for Fibre Channel on Solaris Release Notes*.
- If you are upgrading to Data ONTAP 7.1 on a storage system that has active Internet SCSI (iSCSI) sessions to Windows hosts running release 1.03 or earlier of the Microsoft iSCSI Initiator, you must do one of the following before performing the upgrade:
 - ◆ Shut down all hosts with active iSCSI sessions to the storage system.
 - ◆ Stop applications on all the hosts that are currently using iSCSI Logical Unit Numbers (LUNs) through the Microsoft iSCSI initiator, and then log off iSCSI sessions using the Microsoft iSCSI Initiator control panel.

For detailed information about these host-related procedures and which procedure is more suitable for your environment, see Bug ID 115034.

- Open Systems SnapVault® Agent 1.0 is incompatible with Data ONTAP 7.1.
If you are upgrading to the Data ONTAP 7.1 release family and you are using Open Systems SnapVault Agent 1.0, you must upgrade your Open Systems SnapVault agent to version 1.1 or later.
- SecureAdmin™ 2.2.1 and earlier software is incompatible with Data ONTAP 6.4 and later.
If your storage system is licensed for SecureAdmin and you are upgrading to Data ONTAP 7.1, you must be running SecureAdmin 3.0 or later.

For more information about upgrade issues, see the *Upgrade Guide*.

If you upgrade from Data ONTAP 6.4.x and use CHAP authentication with iSCSI

If you upgrade from the Data ONTAP 6.4 release family and you have Challenge Handshake Authentication Protocol (CHAP) configured for iSCSI, the CHAP configuration from the previous release is not saved.

The CHAP configuration file in Data ONTAP 6.5 and later uses a new format that is not compatible with the CHAP configuration file format of previous releases. When you upgrade, you must use the `iscsi security` command to reconfigure CHAP settings. For information about using the `iscsi security` command, see the *Block Access Management Guide*.

If you upgrade systems running SnapMirror

If you are upgrading Data ONTAP on storage systems that are running the SnapMirror® software and are using volume SnapMirror replication, it is important that you upgrade storage systems that have SnapMirror destination volumes before you upgrade storage systems that have SnapMirror source volumes. This is necessary because when using SnapMirror volume replication, the destination volume must run under a version of Data ONTAP equal to, or later than, that of the SnapMirror source volume.

Also, be aware that synchronous SnapMirror is not allowed to achieve synchronous mode (In-Sync) when the versions of Data ONTAP do not match. If the destination is upgraded first, SnapMirror will automatically do per-minute updates instead of synchronous updates until the source is upgraded to the same version of Data ONTAP. Once both source and destination are using the same version of Data ONTAP, synchronous mode is achieved automatically.

For further important information about updating storage systems that are running SnapMirror, see the *Upgrade Guide*.

For more information about prerequisites for running SnapMirror, see the *Data Protection Online Backup and Recovery Guide*.

If you are running DataFabric Manager with a Business Continuity License enabled

If you are running DataFabric Manager with a Business Continuity License enabled, you must upgrade to DataFabric Manager 3.0.1R1 or later. Not doing so will cause SnapVault relationship updates to fail and display the following error message:

```
"destination requested snapshot that does not exist on the source"
```

For more information about the bugs related to this recommendation, see Bug ID 128767 and Bug ID 132355.

If you have a SnapLock Compliance license

Note

There are two types of Snaplock Licenses in Data ONTAP: SnapLock Compliance and SnapLock Enterprise. When you display licenses for your storage system, the Snaplock Compliance license is listed as `snaplock` and the Snaplock Enterprise license is listed as `snaplock_enterprise`. This information applies to Snaplock Compliance licenses only.

If you upgrade to any Data ONTAP version released on or after March 7, 2005, you must obtain a unique updated SnapLock Compliance license code from the Protocol Licenses page. Previous SnapLock Compliance license codes have been replaced with the updated SnapLock Compliance license codes on this page.

Important

If you upgrade a FAS or NearStore storage system to any Data ONTAP version released on or after Mar 7, 2005 without changing the license code, the attributes and SnapLock protection on already existing SnapLock files (and SnapLock volumes) will not be affected in any way. But because the old license is no longer functional, **you will not be able to commit any new files to SnapLock protected status until the license code is updated**, nor will you be able to

create new SnapLock volumes.

Legal Information

Last updated: 21-Mar-2006 13:25

Known Problems and Limitations

This section describes potential problems and limitations identified with the Data ONTAP® 7.1 release family:

- Manageability issues
 - ◆ 4 Gb HBA is not recognized by earlier diagnostics software (new in 7.1.0.1)
 - ◆ Synchronous SnapMirror and FlexVol volumes
 - ◆ SSH Secure Shell/SSH Tectia client does not work properly unless forwarding is disabled
 - ◆ Maximum number of SSH sessions
 - ◆ Long-running commands invoked using SSH may be terminated
 - ◆ SSH authentication agent forwarding is not supported
 - ◆ Pseudo-terminals are not supported for SSH
 - ◆ PuTTY command line editing does not work properly
 - ◆ Non-local users cannot use login protocols
 - ◆ FilerView does not support roles and capabilities for all tasks
 - ◆ No secondary image on systems with 32 MB CompactFlash cards
 - ◆ Reversion cannot take place during inode-to-pathname initialization
- Protocol issues
 - ◆ NFSv4 client compatibility
 - ◆ NFS configuration issue for Hummingbird with Kerberos
 - ◆ Client notification messages in Windows domains require NetBIOS
 - ◆ Unsupported Windows features in the file serving environment
 - ◆ Do not use `vlan delete -q` with `ipsec`
 - ◆ iSNS service and Microsoft iSNS Server v.3.0
 - ◆ Enable caching with NIS lookup
 - ◆ Group Policy Objects (GPOs) are applied differently on storage systems and Windows systems
- Data protection issues
 - ◆ Stagger Snapshot copy schedules to avoid transfer conflicts
 - ◆ Synchronous SnapMirror and storage system performance
 - ◆ `vscan` feature does not support NIS authentication
 - ◆ Compatibility with SnapDrive and SnapManager
 - ◆ FlexVol volumes cannot be migrated using SnapMover
 - ◆ Potentially reduced performance for IPSec traffic
- Storage resource management issues
 - ◆ Default quota requirement
 - ◆ Changing the IP address of a FlexCache origin storage system
 - ◆ Partition alignment problems cause an iSCSI LUN performance problem
 - ◆ CFO partner node's SSL certificate is used after takeover and giveback
 - ◆ LUNs in FlexCache volumes
 - ◆ Qtree path not shown in quota report for new qtrees
 - ◆ Change in `sysstat -x` command output (new in 7.1.0.1)

Manageability issues

4 Gb HBA is not recognized by earlier diagnostics software

If you want to run NetApp diagnostics software on the 4 Gb target HBAs, you must use diagnostics version 4.6.5 or later. If you run an earlier version of diagnostics software on a FAS3000 series system running Data ONTAP 7.1.0.1, you will see an error message indicating that the 4 Gb HBA is an unrecognized device. Diagnostics version 4.6.5 is available from the Service Image Archive for Diagnostics and Common Firmware Executable (on the NOW site at http://now.netapp.com/NOW/download/tools/serviceimage/archive_fas3000.shtml).

Synchronous SnapMirror and FlexVol volumes

A storage system cannot be both the source of a synchronous SnapMirror® relationship using FlexVol" volumes and the destination of another synchronous SnapMirror relationship using FlexVol volumes.

SSH Secure Shell/SSH Tectia client does not work properly unless forwarding is disabled

If you use the SSH Tectia (Secure Shell) client from SSH Communications Security to access your storage system, you must disable all forwarding. If you do not disable forwarding, in non-interactive mode the client authenticates but does not run the specified command, and the SSH session remains in use until the storage system is rebooted.

Maximum number of SSH sessions

Data ONTAP supports a maximum of 12 SSH sessions.

Long-running commands invoked using SSH may be terminated

If you invoke a command that takes longer than one minute to complete using the non-interactive SSH protocol, it may be terminated before it completes. To avoid this issue, use the interactive SSH protocol or the less secure non-interactive **rsh** protocol.

SSH authentication agent forwarding is not supported

Data ONTAP does not support SSH authentication agent forwarding.

Pseudo-terminals are not supported for SSH

SSH pseudo-terminals such as **pty** are not supported by Data ONTAP. This may cause some clients to produce a message stating that "Server refused to allow pty". Though generally benign, this limitation might cause certain client shortcuts to fail.

PuTTY command line editing does not work properly

If you use PuTTY to access your storage system, and you are using SSH2, you might see the message "Server refused to allow pty" and command line editing features might not work properly. If this happens, use SSH1. To use SSH1, set the storage system **ssh2.enable** option to Off and set the **ssh1.enable** option to On.

Non-local users cannot use login protocols

Non-local users, or users added with the **useradmin domainuser add** command, cannot log in using the login protocols (telnet, console, rsh, ssh, or http-admin) to a system running Data ONTAP. Non-local users can log in only by using the Windows RPC mechanism, and can use only the API capability once they are logged in. This is true regardless of the capabilities associated with any NetApp system group the non-local user has been placed in.

FilerView does not support roles and capabilities for all tasks

For some tasks, the FilerView® administration tool accesses the storage system as root, regardless of what user name you used to log in to FilerView. This means that when you use FilerView, you may not be limited by which capabilities are associated with your user name.

To prevent a user from using FilerView, assign that user only to groups that do not have the **login-http-admin** capability.

No secondary image on systems with 32 MB CompactFlash cards

Generally, during a Data ONTAP upgrade on CompactFlash-based systems, the **download** command copies a new boot image to the CompactFlash card and attempts to back up the existing boot image as a secondary boot image. Beginning with Data ONTAP version 6.5, two boot images cannot fit on 32-MB CompactFlash media; therefore a secondary CompactFlash boot image is not available on systems with a 32-MB CompactFlash card. Although the secondary image is no longer available, the alternative mechanisms of booting over a network (netboot) or with a diskette for recovery are more than adequate. It is unlikely that a secondary image will be required.

If your storage system currently has a 32-MB CompactFlash card and you want to upgrade to a larger card, 256-MB cards are available from NetApp. For your convenience, you can order a 256-MB CompactFlash card using the existing Return Material Authorization (RMA) process. To obtain the card, submit a request at the Submit RMA/Return Request page (on the NOW site at <https://now.netapp.com/eservice/submitRMA.do?moduleName=RMA>).

Replacement 256-MB CompactFlash cards are provided for the purpose of upgrading to Data ONTAP 6.5 or later and are available through Best Effort delivery from regional depots only.

Note

NetApp storage systems support only CompactFlash media distributed by Network Appliance and its partners.

Reversion cannot take place during inode-to-pathname initialization

When you upgrade to Data ONTAP 7.1, inode-to-pathname information is written to each existing volume. You cannot revert to an earlier release while the system is being scanned to initialize the inode-to-pathname information. Before proceeding with the reversion, you must do one of the following:

- Wait until the scan for inode-to-pathname information completes.

This can take many hours, depending on the number of inodes and volumes on your system.

- Abort the scan.

To abort the inode-to-pathname scan, complete the following step.

Enter the following command:

```
vol options no_i2p on
```

Result: Inode-to-pathname translation is disabled immediately and the reversion can proceed.

Note

Because any inode-to-pathname information is removed during a reversion, reverting to an earlier release can take several hours, depending on the number of inodes and volumes on your system, and whether the scan for inode-to-pathname information has been completed.

Protocol issues

NFSv4 client compatibility

If you use NFSv4

When your NFSv4 clients are in a different domain than your NetApp® device is in, you might need to enter the client domain name as the value for the Data ONTAP option **nfs.v4.id.domain**, in order to provide mapping for file ownership and group membership. For more information about mapping options, see RFC 3530 and your client operating system documentation.

If you have any client that needs to access a storage system using NFSv4, ensure that the Data ONTAP option **nfs.v4.enable** is set to On. In new installations, this option is set to off by default.

If you do not use NFSv4

If you do not use NFSv4, ensure that the Data ONTAP option **nfs.v4.enable** is set to Off.

For more information about NFSv4, see the *File Access & Protocols Management Guide*.

NFS configuration issue for Hummingbird with Kerberos

The Data ONTAP option **nfs.mount_rootonly** should be set to Off for implementations that require support for Hummingbird® software using Kerberos v5 authentication.

Client notification messages in Windows domains require NetBIOS

The Windows client notification feature used for client messaging, shutdown notices, and vscan alerts requires NetBIOS over TCP to be enabled in Data ONTAP. On Windows clients, NetBIOS over TCP must be enabled and the Windows Messenger service must be running. (Windows 2003 and Windows XP SP2 clients have messaging disabled by default.)

Unsupported Windows features in the file serving environment

This release does not support every available Windows 2000 and Windows XP feature. For example, this release does not support the following:

- Encrypting File System (EFS)
- Logging of NT File System (NTFS) events in the change journal
- File Replication Service (FRS)
- Microsoft® Windows Indexing Service
- Remote storage through Hierarchical Storage Management (HSM)
- Local user account creation from the User Manager or Microsoft Manager Console
- Quota management from Windows 2000 clients
- Windows 2000 quota semantics
- The LMHOSTS file
- NT File System (NTFS) native compression

Do not use vlan delete -q with IPsec

NetApp recommends you delete VLAN interfaces one by one (that is, do not use **vlan delete -q**) when ipsec is enabled.

iSNS service and Microsoft iSNS Server v.3.0

Data ONTAP 7.1 and later works by default with releases earlier than v.3.0 of the Microsoft iSNS server. If you want to use v.3.0 of the Microsoft iSNS server, set the **iscsi.isns.rev** option to 22:

options iscsi.isns.rev 22

For more information, see iSNS Service Incompatibility with Microsoft iSNS Server v.3.0.

Enable caching with NIS lookup

If you use NIS for group lookup services, disabling NIS group caching can severely degrade performance. Whenever you enable NIS lookups (**nis.enable**), NetApp recommends that you also enable caching (**nis.group_update.enable**). Failure to enable these two options together could lead to timeouts as CIFS clients attempt authentication.

Group Policy Objects (GPOs) are applied differently on storage systems and Windows systems

Data ONTAP 7.1 and later releases support Group Policy Objects (GPOs) that are relevant to storage system management. However, Event Log and Audit (Local Policies) GPOs are applied differently on NetApp storage systems than on Windows systems. For more information, see the *File Access & Protocols Management Guide*.

Data protection issues

Stagger Snapshot copy schedules to avoid transfer conflicts

Data ONTAP provides a default Snapshot copy schedule for each volume that can be modified using the **snap sched** command. The **snap sched** command configures a per-volume schedule that creates, rotates, and deletes hourly, nightly, and weekly Snapshot copies. If either the SnapMirror or SnapVault® feature is scheduled to perform Snapshot management at the same time as a **snap sched** activity, then the Snapshot management operations scheduled using the **snap sched** command might fail with syslog messages such as "Skipping creation of hourly snapshot copy," and "Snapshot copy already exists."

To avoid this condition, stagger your Snapshot copy update schedules so that SnapMirror activity does not begin or end at the exact time a **snap sched** operation attempts to create a Snapshot copy. Additionally, if **snap sched** Snapshot copies conflict with SnapVault activity, use the **snapvault snap sched** command to configure equivalent schedules.

For more information about the SnapMirror and SnapVault features, and for a detailed description of how to use the **snap sched** command, see the *Data Protection Online Backup and Recovery Guide*.

See Bug ID 88184 in Bugs Online for more information.

Synchronous SnapMirror and storage system performance

The synchronous mode of SnapMirror will have an impact on the performance of a storage system. This impact is dependent on the power of your storage system, its load, and the number of simultaneous synchronous SnapMirror relationships. To keep this impact under control, no more than eight simultaneous synchronous SnapMirror relationships are supported.

Please engage your professional services consultant for help with best-practice configuration for synchronous SnapMirror.

vscan feature does not support NIS authentication

The storage system anti-virus vscan feature requires NTLM or Kerberos authentication; it does not support Network Information Service (NIS) authentication. The storage system validates any vscan server which connects to the storage system, and it requires the vscan server to connect as a user who is in the storage system's Backup Operators group.

See Bug ID 139111 in Bugs Online for more information.

Compatibility with SnapDrive and Snap Manager

This version of Data ONTAP is not supported by all versions of NetApp software for Windows clients. Before installing or upgrading to this version of Data ONTAP, make sure that the SnapManager® and SnapDrive™ versions you are running or plan to install are compatible with this release. For more information about supported versions of Data ONTAP for client software, see the client software's Description page on the NOW site.

FlexVol volumes cannot be migrated using SnapMover

Data ONTAP 7.1 and later releases do not support migrating FlexVol volumes or aggregates containing these volumes using SnapMover software. You can use SnapMover to migrate only traditional volumes between clustered nodes.

Potentially reduced performance for IPsec traffic

Data ONTAP 7.1 and later releases do not support hardware-assisted IPsec encryption and instead only uses software encryption. If your storage system includes hardware-assisted encryption, and you use IPsec encryption for high volumes of traffic, you might see reduced throughput for the IPsec encrypted traffic.

Storage resource management issues

Default quota requirement

You should create default user, group, and tree quotas for any volume with quotas enabled. Without these quotas, you might see very high CPU utilization.

Changing the IP address of a FlexCache origin storage system

To change the IP address of a storage system that is currently serving as the origin system for one or more FlexCache volumes, you must first delete all FlexCache volumes backed by the volumes on that system, then change the IP address, then recreate the FlexCache volumes.

Partition alignment problems cause an iSCSI LUN performance problem

Under some circumstances you will get poor performance on iSCSI LUNs used by Linux hosts because of partition alignment problems. See Knowledgebase article 8190 for more information.

CFO partner node's SSL certificate is used after takeover and giveback

If you have two clustered nodes, each with its own certificate, and one node takes over the other node, then after you issue the **cf giveback** command, both nodes may present the certificate for the takeover node. If this happens, restart SSL on the node that was taken over.

LUNs in FlexCache volumes

Although you cannot use SAN access protocols to access FlexCache volumes, you might want to cache a volume that contains LUNs along with other data. When you attempt to access a directory in a FlexCache volume that contains a LUN file, the command sometimes returns "stale NFS file handle" for the LUN file. If you get that error message, repeat the command.

Qtree path not shown in quota report for new qtrees

In the quota specifier field of quota reports, the fully qualified path to qtrees created in Data ONTAP 7.0 and newer is not displayed. For qtrees created in Data ONTAP 6.x and older, the fully qualified path is displayed.

Change in **sysstat -x** command output

In Data ONTAP 7.1 and later releases, the DAFS column is no longer displayed in the **sysstat -x** command output. Note that any scripts that currently depend on **sysstat -x** command output might need to be revised.

Legal Information

Last updated: 21-Mar-2006 15:39

Changes to published documentation

This section corrects or adds to information published in the Data ONTAP 7.1 manuals.

- Changes to the System Configuration Guide
- Changes to the Storage Management Guide
- Change to the Block Access Management Guide for iSCSI and FCP

Changes to the System Configuration Guide

Information about expansion slot assignments for 4 Gb target HBAs can be found in the *System Configuration Guide*. To view this information, select "Release 7.1" from the ONTAP menu; Release 7.1.0.1 does not appear in the list of Data ONTAP releases. Then select your "FAS3050" or "FAS3020" and "Expansion slots/cards."

Changes to the Storage Management Guide

Displaying disk space usage on an aggregate

The section titled "Displaying disk space usage on an aggregate" should read as follows:

To display how much disk space is used in an aggregate, use the **df -A aggr_name** command.

The **aggr show_space** command is not supported in this release of Data ONTAP.

Change to the Block Access Management Guide for iSCSI and FCP

The following passage should be added to Chapter 13, "Managing the Fibre Channel SAN."

Changing the adapter speed

Use the **fcv config** command to change the FC adapter speed. These are the available speeds:

- Autonegotiate (default)
- 1 Gb
- 2 Gb
- 4 Gb

Follow these steps to change the speed.

Step	Action
1	Set the adapter to down (to be offline) using the following command: <pre>fcv config adapter down</pre> Note: This may temporarily interrupt FCP service on the adapter. Example <pre>: device1> fcv config 2a down : Wed Jun 15 14:04:47 GMT [device1: : scsitarget.ispfct.offlineStart:notice]: : Offlining Fibre Channel target adapter 2a. : Wed Jun 15 14:04:47 GMT [device1:</pre>

	: scsitarget.ispfct.offlineComplete:notice]: Fibre Channel : target adapter : 2a offlined.
2	Enter the following command: fcv config adapter speed [auto 1 2 4] Example : device1> fcv config 2a speed 4
3	Enter the following command: fcv config adapter up Result The new adapter speed is set and the adapter is online again. Example : device1> fcv config 2a up : Wed Jun 15 14:05:04 GMT [device1: scsitarget.ispfct.onlining:notice]: : Onlining Fibre Channel target adapter 2a. : device1> fcv config : 2a: ONLINE Loop No Fabric : host address 0000da : portname 50:0a:09:81:96:97:a7:f3 nodename : 50:0a:09:80:86:97:a7:f3 mediatype auto speed 4Gb

Note

Although the **fcv config** command displays the current adapter speed setting, it does not necessarily display the actual speed at which the adapter is running. For example, if the speed is set to auto, the actual speed may be 1 Gb, 2 Gb, or 4 Gb. To view the actual speed at which the adapter is running, use the **show adapter -v** command and examine the Data Link Rate value (shown in bold below).

Example

```
device1> fcv show adapter -v
Slot: 5a
Description: Fibre Channel Target Adapter 5a (Dual-channel, QLogic 2312 (2352) rev. 2)
Status: ONLINE
Host Port Address: 010200
Firmware Rev: 4.0.18
PCI Bus Width: 64-bit
PCI Clock Speed: 33 MHz
FC Nodename: 50:0a:09:80:87:69:27:ff (500a0980876927ff)
FC Portname: 50:0a:09:83:87:69:27:ff (500a0983876927ff)
Cacheline Size: 16
FC Packet Size: 2048
SRAM Parity: Yes
External GBIC: No
Data Link Rate: 4 GBit
Adapter Type: Local
Fabric Established: Yes
Connection Established: PTP
Mediatype: auto
Partner Adapter: NoneStandby: No
Target Port ID: 0x1
```

Data ONTAP 7.1.0.1 Release Notes

Slot: 5b
Description: Fibre Channel Target Adapter 5b (Dual-channel, QLogic 2312 (2352) rev. 2)
Status: ONLINE
Host Port Address: 011200
Firmware Rev: 4.0.18
PCI Bus Width: 64-bit
PCI Clock Speed: 33 MHz
FC Nodename: 50:0a:09:80:87:69:27:ff (500a0980876927ff)
FC Portname: 50:0a:09:84:87:69:27:ff (500a0984876927ff)
Cacheline Size: 16
FC Packet Size: 2048
SRAM Parity: Yes
External GBIC: No
Data Link Rate: 4 GBit
Adapter Type: Local
Fabric Established: Yes
Connection Established: PTP
Mediatype: auto
Partner Adapter: None
Standby: No
Target Port ID: 0x2

Legal Information

Last updated: 21-Mar-2006 16:49

Where to find product documentation and other information

You can access documentation for all NetApp® products on the NetApp on the Web" (NOW) site at now.netapp.com. You can also find other product information resources there, such as technical reports and white papers.

Documentation Roadmap

The *Documentation Roadmap*, which you can find on the Data ONTAP 7.1.0.1 Documentation page, lists NetApp documents and NOW pages (including such things as tools and technical reports) that can help you complete the following major tasks:

- Installing new NetApp systems
- Configuring new NetApp systems
- Upgrading Data ONTAP® on NetApp systems
- Managing NetApp systems
- Diagnosing and troubleshooting problems
- Customizing or automating processes

Finding documentation on NOW

To find the documentation roadmap and other documentation for the Data ONTAP 7.1 release family, as well as the Release Notes for the latest release, follow the Documentation links on the NOW" site to the Information Library page and click the links for Data ONTAP 7.1 documentation (for all releases in the Data ONTAP 7.1 release family) and the Release Notes for your specific release.

You can use this path of links from the NOW home page to the Data ONTAP 7.1.0.1 Documentation page:

Technical Assistance and Documentation > Access & Order Product Documentation > Data ONTAP > Data ONTAP for Filer/NearStore > All documents (HTML & Acrobat) for Data ONTAP 7.1.0.1.

Searching online information

The NOW Natural Language PowerSearch tool on the Service and Support page on the NOW site allows you to search the following sources of information:

- Product documents
- Knowledgebase solutions
- Bugs online
- NOW forums
- Tools and other documentation
- Partner knowledgebases

Legal Information

Last updated: 21-Mar-2006 13:26