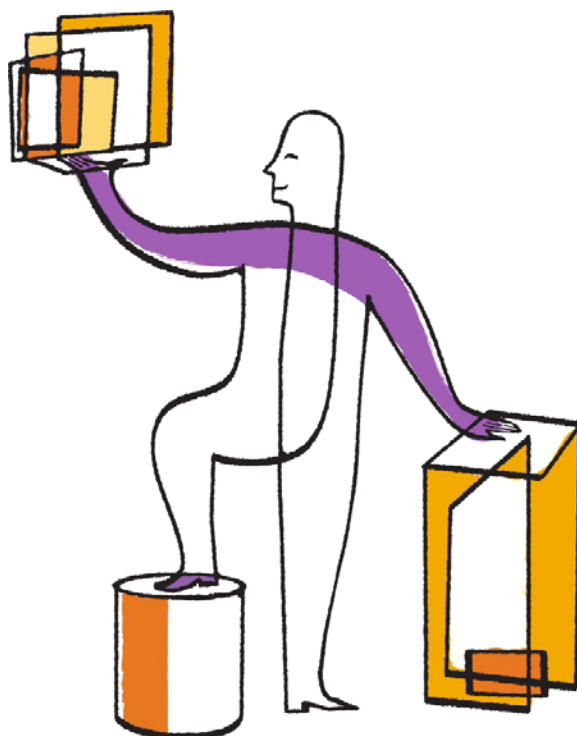




NetApp®

NetApp® SANtricity® Web Services Proxy 1.2

User Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1-(888) 463-8277
Web: <http://www.netapp.com>
Feedback: doccomments@netapp.com

Part number: 215-09994_A0
Release date: April 2015

Table of Contents

Overview of the NetApp Web Services Proxy	1
New in This Release	1
Abbreviations, Acronyms, Terms, and Definitions	1
NetApp Web Services Proxy Interfaces	2
NetApp Web Services Proxy APIs	2
Cross-Domain Resource Sharing	2
Symbol Web	2
Compatible Storage Arrays and Controller Firmware	2
IP Support	3
NVSRAM File Name Constraints	3
MEL Events Cache Size	3
Web Services Proxy Configuration Files	3
Default Configuration Files	3
Configuring the Optional cors.cfg File	4
Configuring the wsconfig.xml File	4
Configuring Polling Intervals	4
Resolving Port Conflicts	5
Configuring the users.properties file	5
Flags and Settings	6
Logging in to Web Services Proxy	6
Login URL Authentication	6
Basic Authentication	6
NetApp Web Services Proxy Security	7
Generating Certificates	7
Generating a Self-Signed Certificate	7
Generating an SSL Certificate	7
File Handles Limit	8
User Roles and Access	8
Adding Storage Arrays	9
Automatically Discovering Storage Arrays	9
Turning Off Automatic Discovery of Storage Arrays	9
Automatic Polling of Volume and Disk Statistics	9
AutoSupport (ASUP)	10
ASUP Schedule	10
Configuring ASUP Delivery Type	10
Enabling and Disabling ASUP Post-Web Services Installation	11
Managing Auto Updates	11
Rolling back to original software	11
Version Numbers	12
Logging in to the API	12
Scaling Up the Number of Managed Arrays	12

Overview of the NetApp Web Services Proxy

The NetApp Web Services Proxy provides access through standard HTTPS mechanisms for configuring management services for NetApp storage arrays. You can install the Web Services Proxy on both Linux machines and Windows machines. As the NetApp Web Services Proxy satisfies client requests by collecting data or executing configuration change requests to a target storage array, the NetApp Web Services Proxy module issues SYMBOL requests to the target storage arrays.

The NetApp Web Services Proxy provides a Representative State Transfer (REST)-style application programming interface (API) for managing NetApp storage array controllers. The API enables you to integrate array management into other applications or ecosystems. The Web Services Proxy Array Manager complements the API as a management and debugging tool. If you are having problems scripting array commands, you can check the status of a storage array in the Array Manager.

New in This Release

This release of the Web Services Proxy adds the following features, functions, and capabilities:

- AutoSupport (ASUP)
- Auto Download of Updates
- REST resource enhancements
 - Configuration of owning controller and cache settings for volumes and thin volumes
 - Online VolumeCopy support
 - Drive tray connectivity endpoint
 - Endpoint for viewing FlashCache information
 - Intelligent ConcatVolumeCandidate selection for increased flexibility in defining Snapshot-related objects
 - Endpoint for viewing ConcatVolumes (repositories)
 - View repository utilization for Snapshot groups, Snapshot views, Async Mirrors, and Legacy-Snapshots
- Hardware and firmware
 - E5600, EF550, and EF560 storage arrays
 - Dual Port FDR 56-Gb InfiniBand
 - Support for controller firmware 8.20

Abbreviations, Acronyms, Terms, and Definitions

The following table shows the abbreviations, acronyms, and terms used in this guide and their definitions.

Abbreviations, Acronyms, Terms	Definitions
API	Application Programming Interface
CORS	Cross-Origin Resource Sharing
FDR	Fourteen Data Rate
JSON	JavaScript Object Notation
REST	Representational State Transfer

NetApp Web Services Proxy Interfaces

The Web Services Proxy provides REST-style interface for accessing common configuration operations and to retrieving basic configuration data, status, and statistics. For more information about the interface, go to the NetApp Web Services Proxy Developer Guide at <https://<nnn.nnn.nnn.nnn>:8443/docs>, where `nnn.nnn.nnn.nnn` represents the host server.

NetApp Web Services Proxy APIs

The Storage Management Web Services Proxy executes commands on the target controller. The REST-style API enables you to manage the following storage system objects:

- MEL events
- Disk drives
- Storage pools
- Volume copy jobs
- Snapshot groups
- Host groups
- Volume I/O statistics
- Snapshot images
- Host groups
- Thin-provisioned volumes
- Volume mappings
- Hardware inventory
- Snapshot volumes
- Host types
- Volumes
- Hosts
- Storage arrays
- Disk statistics

For a complete list of all endpoints, see the API documentation.

Cross-Domain Resource Sharing

Cross-domain resource sharing (CORS) is handled by a `cors.cfg` file in the `working` directory of the web server as specified in the `wsconfig.xml` file. The CORS configuration is open by default, so cross-domain access is not restricted.

NOTE: If no configuration file is present, CORS is open.

Symbol Web

Symbol Web is a URL in the REST API, but it gives access to almost all symbol calls. The symbol function is the part of the following URL:

`http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function`

Compatible Storage Arrays and Controller Firmware

Web Services Proxy is compatible with the following NetApp storage arrays and controller firmware versions. The following table shows the compatible storage arrays and control firmware.

Storage Array	Interfaces	Controller Firmware
NetApp E2600	6Gbps iSCSI 8Gbps FC 6Gpbs SAS	7.84 7.86 8.10
NetApp E2700	10Gbps iSCSI 16Gbps FC 12Gpbs SAS	7.84 7.86 8.10
NetApp E5400 NetApp EF540	10Gbps iSCSI 8Gbps FC 6Gbps SAS	7.84 7.86 8.10
NetApp E5500 NetApp EF550	10Gbps iSCSI 16Gbps FC 12Gbps SAS FDR 56Gbps IB	7.84 7.86 8.10

Storage Array	Interfaces	Controller Firmware
NetApp E5600 NetApp EF560	10Gbps iSCSI 16Gbps FC 56Gbps IB 12Gbps SAS	

IP Support

Web Services Proxy supports both the IPv4 protocol and the IPv6 protocol.

NOTE: The Ipv6 protocol might not work in some situations when the Web Services Proxy is attempting to automatically discover management address from the controller configuration, such as in IP address forwarding or when Ipv6 is enabled on the storage arrays but not on the server.

NVSRAM File Name Constraints

The Web Services Proxy uses NVSRAM file names to accurately identify version information. Therefore, you cannot change NVSRAM filenames when they are to be used with the Web Services Proxy. The Web Services Proxy might not recognize a renamed NVSRAM file as a valid firmware file.

MEL Events Cache Size

The default cache size is 8192 events. The approximate data usage for the MEL events cache is 1MB for each 8192 events. Therefore, by retaining the defaults, cache usage should be approximately 1MB for a storage array.

Web Services Proxy Configuration Files

After you have installed the NetApp Web Service, you can either accept the default NetApp Web Services Proxy settings or modify them to meet the unique operating and performance requirements for your environment.

Default Configuration Files

The Web Services Proxy installs the following two default configuration files:

- `wsconfig.xml`
- `users.properties`

By default, the files are installed in the following locations:

- Windows – `C:\Program Files\NetApp\SANtricity Web Services Proxy`
- Linux – `/opt/netap/ santricity_web_services_proxy`

The following table shows the default locations and configuration files.

Default Directory Locations	Description
<install root>/wsconfig.xml	The primary configuration file for the Web Services Proxy
<install root>/working/users.properties	Web Services Proxy password files. For more information, go to Configuring the users.properties File .

To restrict Cross-Origin Resource Sharing (CORS) access, you can install and configure the optional `cors.cfg` file. For more information about the `cors.cfg` file, go to [Configuring the Optional cors.cfg File](#).

Configuring the Optional cors.cfg File

Cross-Domain Resource Sharing (CORS) is handled by the `cors.cfg` file in the working directory in the web service, as specified by the `wsconfig.xml` file. The CORS configuration is open by default, so cross-domain access is not restricted. If no configuration file is present, CORS is open. If the `cors.cfg` file is present, it is used. If the `cors.cfg` file is empty, you cannot make a CORS request.

To configure CORS settings, add lines to the `cors.cfg` file. Each line in the CORS configuration file is a regular expression pattern to match. The origin header must match a line in the `cors.cfg` file. If any line pattern matches the origin header, the request is allowed. The complete origin is compared, not just the host element. This allows requests to be matched not only on the host, but also according to protocol, such as the following:

- Match localhost with any protocol—`*localhost*`
- Match localhost for HTTP only—`https://localhost*`

Configuring the wsconfig.xml File

The `wsconfig.xml` file controls most of the service. Use the `wsconfig.xml` to configure the HTTP and HTTPS ports and various directory paths.

Configuring Polling Intervals

To enable polling and the analyzed URLs, add the following lines to the `wsconfig.xml` file, where `nn` is the number of seconds for the interval between polling requests:

```
<env-entries>
<env key="stats.poll.interval">nn</env>
</env-entries>
```

Example

```
<env-entries>
<env key="stats.poll.interval">60</env>
</env-entries>
```

- Polling starts at 60-second intervals; that is, the system requests that polling starts 60 seconds after the prior polling period was completed, regardless of the duration of the prior polling period. It does *not* mean that polling starts every 60 seconds.
- All the statistics are time-stamped with the exact time they were retrieved. The system uses the time stamp or time difference on which to base the 60-second calculation.

NOTE: The statistics are cached in memory, so you might see an increase of about 1.5 megabytes of memory-use for each array.

Resolving Port Conflicts

When the Web Services Proxy is running, but another application is available at a defined address or port, a port conflict can occur. To resolve a port conflict do the following:

1. Change the port or ports configured in the `wsconfig.xml` file.
2. Restart the service.

The following table shows the attributes of the NetApp Web Server configuration file that control HTTP ports and HTTPS ports.

Name	Description	Parent Node	Attributes	Required
config	The root node for the config	Null	Version - The version of the config schema is currently 1.0.	Yes
sslport	The TCP port to listen for SSL requests. Defaults to 8443	config	Clientauth	No

To configure the `wsconfig.xml` file, perform these actions:

1. Open a terminal window, and log in to the NetApp Web Services Proxy as root.
2. Navigate to the `/opt/netapp/web/service` directory.
3. With a text editor, open the `wsconfig.xml` file.
4. Make the necessary changes.
5. Save the file.
6. Close the file.

The following screenshot displays an example of a sample screen output of the `wsconfig.xml` file.

```
<?xml version="1.0" encoding="UTF-8"?>
<config version="1">

  <!-- non-ssl port if not specified, no listener is made-->
  <sslport clientauth="request">8443</sslport>
  <!-- comma generated list of protocols Possible values: SSLv3,TLSv1,TLSv1.1-->
  <exclude-protocols>SSLv3</exclude-protocols>

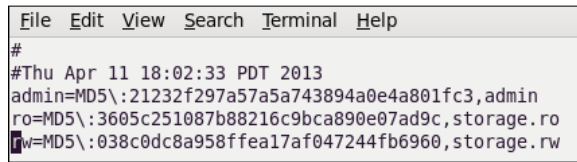
  <port>8080</port>
  <workingdir>C:\Program Files\NetApp\SANtricity Web Services Proxy\working</workingdir>
```

Configuring the `users.properties` file

The `users.properties` file contains user authentication information, including user names, passwords, and roles. The file is in the `/opt/netapp/web/service/working` directory. For detailed information about user names, passwords, and roles, go to [User Roles and Access](#).

When you edit the `user.properties` file, type the password as plain text. Then use the `securepasswordcs` command line utility to encrypt the passwords. The utility is installed in the base install directory for the Web Services Proxy.

The following screenshot displays an example of the default `users.properties` file accessed through a text editor.

A screenshot of a text editor window with a menu bar (File, Edit, View, Search, Terminal, Help). The text content is as follows:

```
#
#Thu Apr 11 18:02:33 PDT 2013
admin=MD5\:21232f297a57a5a743894a0e4a801fc3,admin
ro=MD5\:3605c251087b88216c9bca890e07ad9c,storage.ro
rw=MD5\:038c0dc8a958ffea17af047244fb6960,storage.rw
```

Flags and Settings

You can edit the following other settings in the Environment Entries section.

```
<env-entries>
```

```
<!-- Enables basic authentication. The user no longer is required to use the
/devmgt/utils/login URL --->
```

```
<env key="enable-basic-auth">true</env>
```

```
<!-- Turns on analyzed stats. The polling interval is really a rest interval
between polling runs. If the user has many arrays with many drives and volumes,
polling runs may take a while.
```

```
<env key="stats.poll.interval">30</env>
```

```
</env-entries>
```

Logging in to Web Services Proxy

Login URL Authentication

This is the default way to log in. The sample code shows, using the cookie that it is set on, when the `/util/login URL` is used.

For reference, the cookie value to pass back to the server is `JSESSIONID`.

Basic Authentication

You can use basic authentication when it is enabled. If you are not logged in, the server returns a basic authentication challenge. To enable basic authentication, add the following lines to the `wsconfig.xml` file.

```
<env-entries>
<env key="enable-basic-auth">true</env>
</env-entries>
```

NetApp Web Services Proxy Security

The NetApp Web Services Proxy uses Secure Sockets Layer (SSL) for security.

Generating Certificates

Generating a Self-Signed Certificate

To enable SSL, add an SSL port designation to the `wsconfig.xml` configuration file. When the server is started with SSL configured, the server looks for the keystore and truststore files.

- If the server does not find a keystore, the server uses the IP address of the first non-loop back IPv4 address that finds to generate a keystore and add a self-signed certificate to the keystore.
- If the server does not find a truststore, or the truststore is not specified, the server uses the keystore as the truststore.

Generating an SSL Certificate

The NetApp Web Services Proxy provides a Java keytool with which to generate an SSL certificate. To generate a signed SSL certificate and export and store it on each client, perform these actions:

Generating an SSL Certificate on the Application Server

After you have generated the certificate and saved it in the application server keystore, you can use the certificate again on the same application server.

1. Remove any auto-generated keystores in the working directory.
2. Stop the server.
3. Run the following command to generate the certificate:

```
keytool -genkeypair -keyalg RSA -keysize 2048 -alias jetty -dname CN=<THE SERVER  
DNS NAME> -keypass changeit -storepass changeit -keystore keystore -ext  
san=ip:<THEIR IP ADDRESS>,dns:<THE SERVER DNS NAME> -validity 999  
<or>  
keytool -genkeypair -keyalg RSA -keysize 2048 -alias jetty -dname CN=servername -  
keypass changeit -storepass changeit -keystore keystore -ext  
san=ip:192.168.1.1,dns:servername -validity 999
```

The following message appears in the terminal window:

```
When prompted for a password, use "changeit", unless you specify a specific one in  
the wsconfig.xml file  
When prompted for your first and last name, use the IP address or DNS name of the  
host, whichever one you plan on using in URLs
```

4. Follow the instructions in the terminal window.
5. Run the following command to export the certificate for signing:

```
keytool -certreq -alias jetty -file mycertreq.cer -keystore keystore -dname  
CN=servername -ext san=ip:192.168.1.1,dns:servername
```

6. Send the certificate request to a certifying authority to be signed.
7. Run the following commands to import the CA certificate and the signed certificate back into your keystore.

```
keytool -import -trustcacerts -alias root -file <CA CERT FILE> -keystore keystore
```

```
keytool -import -trustcacerts -alias jetty -file <signed cert from ca> -keystore  
keystore
```

8. Restart the server.
9. Save the certificate in your keystore.

Generating an SSL Certificate on an Application Client

If you do not already have the certificate, import it from the certifying authority. Follow the prescribed import process for your specific operating system and web browser.

File Handles Limit

As a security measure, most operating systems limit the number of open file handles that a process or a user can have open at one time. Especially in Linux environments, where open TCP connections are considered to be file handles, it is very easy for the Web Services Proxy to exceed this limit. The fix is system dependent, so you should refer to your operating system's documentation for how to raise this value.

User Roles and Access

User access to the NetApp Web Services Proxy is based on user roles and their corresponding levels. Only the Read-Write user role can access the Array Manager and the array tree. The Read-Write role enables you to perform any action to a storage array in the array tree in the Array Manager.

- The initial user role is `rw`.
- The password is `rw`.

The following file contains the user IDs, user roles, and passwords:

```
/opt/netapp/websevice/data/config/users.properties
```

User names, passwords, and roles are in the following sequence:

```
user=encryptedpassword,storage.role
```

For more information about configuring passwords, go to [Configuring the wsconfig.xml File](#).

Adding Storage Arrays

Automatically Discovering Storage Arrays

By default, you need to provide only one management IP address to add an array. The server automatically discovers all management paths when the paths are not configured or they are configured and rotatable.

NOTE: If you attempt to use an Ipv6 protocol to automatically discover storage arrays from the controller configuration after an initial connection has been made, the process might fail. Possible causes for the failure include during IP address forwarding or IPv6 is enabled on the Storage Systems but it is not on enabled on the server.

Turning Off Automatic Discovery of Storage Arrays

When the paths are configured, but not configured so that the server can route to the addresses, intermittent connection errors happen. If you cannot set the IP addresses to be routable from the host, you can turn off auto discovery. To turn off auto discovery, modify the following lines in the `wsconfig.xml` file.

```
<env key="autodiscover.ipv6.enable">false</env>
<env key="autodiscover.ipv4.enable">false</env>
```

Automatic Polling of Volume and Disk Statistics

The REST service provides the ability to set up an automatic polling of volume and disk statistics. To enable automatic polling, modify the `wsconfig.xml` file normally located in the `webserver` directory. The new service will poll for all disk and volume statistics on the storage array registered with the service.

This feature does not change the behavior of the URLs for current disk and volume statistics. These URLs continue to retrieve the statistics when they are called. However, the user has the option to add the `usecache=true` query string to the end of the URL to retrieve cached statistics from the last poll. Using cached results greatly increases the performance of statistics retrieval. However, multiple calls at a rate equal to or less than the configured polling interval cache will retrieve the same data.

Two new URLs have been added to a storage array:

- `analysed-drive-statistics/{optional list of disk ids}`
- `analysed-volume-statistics/{optional list of volume ids}`

These URLs retrieve analyzed statistics from the last poll and are only available when polling is enabled. These URLs provide the following input-output data:

- Operations per second
- Throughput in megabytes per second
- Response times in milliseconds

These calculations are based on the differences between statistical polling iterations, which are the most common measures of storage performance. These statistics are preferable to unanalyzed statistics.

NOTE: When the system starts, there is no previous poll to use to calculate the data, so it is based off cumulative data. In addition, if the cumulative counters are reset, the next polling cycle will have unpredictable numbers for the data.

AutoSupport (ASUP)

The AutoSupport (ASUP) feature collects data in a customer support bundle and automatically sends the message file to Technical Support for remote troubleshooting and problem analysis. ASUP automatically transmits messages to NetApp based on manual and schedule based criteria. Each ASUP message is a collection of log files, configuration data, state data, and performance metrics.

The ASUP feature transmits the following files to the NetApp technical support team:

File Name	Description
x-headers-data.txt	A .txt file containing the X-header information
manifest.xml	An .xml file detailing the contents of the message
arraydata.xml	An .xml file containing the list of client persisted data
appserver-config.txt	A .txt file containing the web server configuration data
wsconfig.txt	A .txt file containing the web server configuration data.
host-info.txt	A .txt file containing information about the host environment
server-logs.7z	A .7z file containing every available webserver log file
client-info.txt	A .txt file with arbitrary key/value pairs for application-specific counters such as method and webpage hits

ASUP Schedule

ASUP transmits data once a week.

Configuring ASUP Delivery Type

HTTPS is the default delivery method for the ASUP feature. Users can configure the ASUP feature to use HTTPS, HTTP, or SMTP delivery methods through the `ASUPConfig.xml` file. To modify the ASUP delivery method, enter one of the following values under `<delivery type="(integer)">` of the `ASUPConfig.xml` file:

- 1 – The default delivery method for the ASUP feature, delivers ASUP data via HTTPS

```
<delivery type="1">
```

- 2 – Delivers ASUP data via HTTP

```
<delivery type="2">
```

- 3 – Delivers ASUP data via SMTP

```
<delivery type="3">
```

Enabling and Disabling ASUP Post-Web Services Installation

The ability to enable or disable the ASUP feature is performed during the initial installation of the Web Services Proxy. If needed, users can enable or disable the ASUP feature post-Web Services installation through the `ASUPConfig.xml` file. To enable or disable the ASUP feature post Web Services installation, enter one of the values under `<asupdata enabled="(Boolean)" timestamp="1428601077263">` of the `ASUPConfig.xml` file:

- `true` – Enables the ASUP feature

```
<asupdata enabled="true" timestamp="0">
```

- `false` – Disables the ASUP feature

```
<asupdata enabled="false" timestamp="0">
```

NOTE: The `timestamp` entry is superfluous.

For more information on enabling and disabling the ASUP feature during the Web Services Proxy installation process, refer to the NetApp SANtricity Web Services Proxy Install Guide.

Managing Auto Updates

Starting with version 1.2, the product can automatically download updates that can be installed the next time the application restarts or on demand using the REST API. You can enable or disable this feature after install by editing the `wsconfig.xml` file. The following key controls the auto update feature:

```
<enable-auto-update>true</enable-auto-update>
```

The value can be `true` or `false`.

When the above value is set to `true`, the software checks for updates, and if there is an update, downloads it. The software checks once a day. The overhead for the checking is extremely low.

To manually download updates and install updates at runtime, use the REST API. For further details, please see the only rest documentation for the URL `v2/upgrade`.

Updates are downloaded in the background and the download has no effect on the system.

After downloading, installing the updates at runtime takes several seconds and causes an interruption in service. This does not happen automatically and only when you request it or on restart.

Rolling back to original software

The updated software is placed the directory `<install root>/working/webapps`.

If the user wishes to go back to the original shipped software, they can remove the war files (*.war) from that directory and either restart the application or use the REST API to reload the software.

The original software is always saved in `<install root>/data/webapps`. Do not remove or replace files in this directory.

Version Numbers

There are actually two version numbers associated with the product:

- The version of the application (01.20.XXXX.XXX)
- The version of the REST API

Version number reported via the `/utils/about` URL and reported in the upgrade URL is the version for the REST API. Unless the user installs a new version of the application with the installer, the application version number will not change. The upgrades are upgrading the REST API component.

Logging in to the API

Web Services Proxy has two default user logins and permission levels:

- Read-write access
 - User ID is: rw
 - Password is rw
- Read-only access
 - User id is: ro
 - Password is ro

To log in, type the following URL in a web browser:

<http://<host:port>/utils/login>

In addition, the user can use "Basic Authentication" to login to the service. If a login session has not been established. A Basic Authentication challenge will be sent to the client.

Scaling Up the Number of Managed Arrays

The default setting for the Web API can handle up to 100 storage systems. If you need to manage more, you must bump the memory requirements for the server. On Windows, this is handled in the `appserver64.init` file.

Change the line `vmarg.3=-Xmx512M`.

On Linux, the line is in the `webserver.sh` look for the line `JAVA_OPTIONS="-Xmx512M"`.

To increase the memory, add 250 MB per 100 extra storage arrays. Please do not add more memory than what you physically have allowing enough extra for your operating system and other applications.

In addition to memory, the application uses network ports for each storage system. Linux and Windows consider network ports as file handles. Because of this, see the section on increasing file handles to allow for more storage systems.

Copyright information

Copyright © 1994-2015 NetApp, Inc. All rights reserved. Printed in the U.S.

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

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

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

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

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

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

Trademark information

NetApp, the NetApp logo, Go Further, Faster, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID-DP, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL are trademarks or registered trademarks of NetApp, Inc. in the United States, and/or other countries. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

Cisco and the Cisco logo are trademarks of Cisco in the U.S. and other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

How to send your comments

You can help us to improve the quality of our documentation by sending us your feedback.

Your feedback is important in helping us to provide the most accurate and high-quality information. If you have suggestions for improving this document, send us your comments by email to doccomments@netapp.com. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277



NetApp