Sun StorageTek™ Compliance Archiving System Policy and Procedures Guide

For Sun StorageTek 5000 NAS Family of Products

Sun Microsystems, Inc.
www.sun.com

Part No. 819-4196-12
August 2006, Revision A

Submit comments about this document at: http://www.sun.com/hwdocs/feedback

Contents

Sun StorageTek Compliance Archiving System Policy and Procedures Guide

This guide provides policies, procedures, guidelines, and recommendations for deploying and configuring a complete compliance solution using a Sun StorageTek™ Compliance Archiving System. This document does not address all of the business practices and policies that are required for a complete compliance solution. It is limited to those related to the Sun StorageTek Compliance Archiving System.

This guide is required reading for any person responsible for administering or servicing the Compliance Archiving System, including but not limited to Sun support personnel.

It is divided into the following sections:

System Overview

The Sun StorageTek Compliance Archiving System is a combination of the Sun StorageTek Compliance Archiving Software and the Sun StorEdge™ 5210 NAS Appliance, or any one of the Sun StorEdge 5310 NAS or StorageTek 5320 NAS appliance or gateway systems.

The system connects directly to a network as quickly and simply as a network printer. It features high-speed RAID controller architecture as well as redundant components that improve data availability. The modular, scalable appliance offers nonstop performance for users who require optimum file-sharing capabilities. It is available in several configurations.

The Sun StorageTek Compliance Archiving Software is license-key enabled extension software that facilitates compliance with the stringent data management and retention requirements of the Securities and Exchange Commission (SEC 240.17a-4). By adhering to these rigorous requirements, the Compliance Archiving System also meets the needs of industries that do not have these mandated requirements, but can benefit from the functionality either to help comply with other regulations (for example, Sarbanes Oxley, Basel II, HIPAA, and 21 CFR 11) or to comply with their own internal rules for document management and retention. You can configure the system for mandatory or advisory enforcement, where mandatory enforcement is designed to meet strict requirements such as SEC240.17a-4 and advisory enforcement can satisfy less stringent requirements such as business governance rules.

Note – Mandatory enforcement is not available for the Sun StorageTek 5320 NAS Gateway System or Sun StorEdge 5310 NAS Gateway System.

Key to facilitating compliance with these regulations is the software application that sits in front of the archive, managing the documents and records and interacting with the end user. For example, the combination of Sun Partner Advantage Program Enterprise Content Management (ECM) applications or Integrated Document Archive and Retrieval Systems (IDARS) applications and the storage provided by the Sun StorageTek Compliance Archiving System helps ensure compliance with data management and retention requirements. Also key to facilitating compliance are the business practices and IT policies that you put in place for a complete compliance solution.

System Description

This section provides a description of the Sun StorageTek Compliance Archiving System.

Components of the Compliance Archiving System

The Sun StorageTek Compliance Archiving System can consist of the Sun StorageTek 5320 NAS Appliance, Sun StorageTek 5320 NAS Gateway System, Sun StorEdge 5310 NAS Appliance, Sun StorEdge 5310 NAS Gateway System, or Sun StorEdge 5210 NAS Appliance. The appliances are mid-tier NAS solutions that provide network-based file services to both UNIX® and Windows clients via standard access protocols (Network File System [NFS] and Common Internet File System [CIFS]). The system is configurable with SCSI, Fibre Channel (FC), Serial Advanced Technology Attachment (SATA) disk drives, or as a Gateway system. It provides many features typically found in network attached storage (NAS) appliances, including integrated NFS and CIFS services, point-in-time file system checkpoints (“snapshots”), clustering for high availability, and many others.

Note – Checkpoint files cannot be restored over write-once, read-many (WORM) files.

The Sun StorageTek 5320 Appliance and Sun StorEdge 5310 NAS Appliance can be scaled to 134 terabytes of raw FC or 224 terabytes of raw SATA RAID-protected storage. The Sun StorEdge 5210 NAS Appliance supports up to three SCSI expansion units for a total capacity of 6.1 terabytes of storage.

Features of the Compliance Archiving System

The compliance extensions to the appliance firmware are designed to provide storage-level assurances regarding the accuracy, integrity, and retention of files. This functionality consists of four major features:

- WORM files
- File retention periods
- Administrative lock-down
- Compliance auditing

For test environments or for deployments with less stringent data retention requirements, a privileged user can configure the advisory version of the Compliance Archiving Software to override some data retention rules.

Compliance WORM Files

The Compliance Archiving System provides support for write-once, read-many (WORM) files. WORM files enforce stronger access controls than the traditional file access semantics provided by the NFS and CIFS protocols. When an application designates a file as WORM, the file becomes permanently immutable and can be deleted only when its retention time has been met. WORM files cannot be modified, extended, or renamed. In addition, WORM files can be deleted only in accordance with the file retention rules described below.

Note that although these files are called “WORM,” in keeping with common parlance for non-rewritable, non-erasable storage, it would be more accurate to call them “permanent read-only” files. The Compliance Archiving System does not restrict the way a file is written or the number of times its contents can be modified before the file is turned into a WORM file.

Note – The appliance supports backup to WORM tape for customers who want to back up WORM files to immutable tape media.

File Retention Periods

The Compliance Archiving Software associates a retention period with each WORM file. A WORM file cannot be deleted until its retention period has expired. Retention periods can be extended, but never decreased. An exception to this is the advisory enforcement compliance option explained in the “Compliance Enforcement Options” on page 5. A new retention period can be assigned to a file whose previous retention period has expired.

Caution – If you or the front-end application that writes files to the volume does not explicitly set a retention period for each file, the default retention period is used.

Administrative Lock-Down

In order to ensure the retention and preservation assurances of WORM files and retention periods, certain system administration features are disabled or restricted on compliance-enabled file system volumes. These restrictions affect functions that could be used to circumvent a file's retention (for example, by deleting the file's volume).

Compliance Auditing

The Compliance Archiving Software retains immutable records of all compliance-related activities that occur on the system. This information includes log records for all attempts to modify or delete WORM files (with or without permission). A full description of the audit trail provided by this service can be found in Chapter 9 of the *Sun StorageTek NAS OS Administration Guide*.

Compliance Enforcement Options

When creating a new file volume, an administrator can choose between the mandatory and advisory levels of retention enforcement.

With mandatory enforcement, it is impossible to delete a WORM file prior to its retention date, to decrease a WORM file's retention time, or to delete a compliance volume.

In contrast, advisory enforcement allows an authorized administrator to override certain rules, including decreasing a WORM file's retention time and deleting a WORM file before its retention date. These operations are logged with the previously described Compliance Auditing feature.

Interaction With Antivirus Applications

When you enable antivirus protection on a compliance-enabled volume, the following cases are handled in a special manner:

- If a file is scanned for viruses before it is retained, the file will be quarantined if it is found to be infected.
- If a retained file is scanned for viruses and found to be infected, access will be denied.

For more information about virus scanning, see Chapter 4 of the *Sun StorageTek NAS OS Administration Guide.*

Physical Configuration Recommendations

This section provides recommendations and guidelines for the physical configuration of a Sun StorageTek Compliance Archiving System.

Physical Security

The physical security of a Compliance Archiving System is an important aspect of data security and retention, since software features cannot protect data against accidental or malicious physical destruction, such as the removal and reformatting of one or more hard drives.

Caution – You must take the appropriate steps to ensure the physical security of the data stored in the Sun StorageTek Compliance Archiving System.

In addition, you should replace the batteries in the RAID Controller and the system BIOS in accordance with Sun's maintenance guidelines.

Connections to RAID Expansion Units

The Sun RAID expansion unit controllers should not be connected to any computer system that is not part of the appliance. This restriction applies to both Fibre Channel and Ethernet connections.

The Compliance Archiving Software runs on the appliance and cannot control or restrict the behavior of other computer systems that might be attached to the RAID controllers (within the RAID expansion unit controller enclosures). If other computers are attached to the RAID controllers, the Compliance Archiving Software will no longer be able to protect WORM files from accidental or malicious corruption.

The only circumstance in which an expansion unit should ever be connected to a computer that is not part of the appliance is for troubleshooting by authorized and trained Sun Service personnel.

For the additional protection of data in transit to and from the Sun StorageTek Compliance Archiving System, consider the use of a dedicated private network for data traffic between the Compliance Archiving System and the servers running the record or document management applications.

Note – Always use the Web Administrator graphical user interface (GUI) to reconfigure a RAID array. Reconfiguring by any other means will void the warranty and might compromise the WORM protection of data files retained by the Sun StorageTek Compliance Archiving Software. For more information, see the online help or *Sun StorageTek NAS OS Administration Guide.*

Software Configuration Recommendations

This section provides recommendations and guidelines for the software configuration of a Sun StorageTek Compliance Archiving System.

Integration With Other Applications

The Sun StorageTek Compliance Archiving System is designed to enforce data retention rules and policies. As a result of this design, some file system operations behave differently on compliance-enabled file systems than they do on standard, non-compliance file systems. To avoid confusion, and to ensure the correct management of retained data, the Sun StorageTek Compliance Archiving Software should be used exclusively by applications that have been explicitly modified to manage file retention using the Sun StorageTek Compliance Archiving Software API. This interface and the unique behavior of compliance-enabled file volumes are described in Appendix C of the *Sun StorageTek NAS OS Administration Guide*.

The Compliance Archiving Software provides two modes of operation:

- Sun standard compliance mode (the default). The API for the default mode is available from Sun.
- Sun emulation compliance mode provides compatibility with the Network Appliance, Inc. SnapLock interface. Emulation mode is provided for customers and partners who have already integrated their solution with SnapLock. The emulation API is defined by and available from Network Appliance. For information about the SnapLock API, contact Network Appliance.

You use the `fsctl` command to change the operating mode. To set the operating mode to run in emulation mode, use the command:

```
> fsctl compliance mode compat
```

If you need to set the mode of operation back to the default operating mode, use the command:

```
> fsctl compliance mode standard
```

System Logs

To provide accurate auditing of system reconfiguration, errors, faults, and other events, it is strongly recommended that you enable persistent system logging. By default, the appliance logs these events only to system memory. As a result, log information is lost when the system reboots. Configure the Sun StorageTek Compliance Archiving System either to store log data on one of its file systems or to send log data to a remote `syslog` server. For instructions on configuring system logging, see “Setting Up Logging” in Chapter 2 of the *Sun StorageTek NAS OS Administration Guide.*

System Auditing

By enabling system auditing, you can record details of when advisory compliance volumes are deleted. Records of volume deletions, in addition to other system events, are captured in audit log files. For instructions on how to enable system auditing, see Chapter 10 of the *Sun StorageTek NAS OS Administration Guide*.

Secure Administrative Access

Remote administrative access to the appliance should be limited to secure protocols. To configure the appliance to limit remote access in this manner, follow the directions in the section “Setting Remote Access Options” in Chapter 12 of the *Sun StorageTek NAS OS Administration Guide*.

Select the Secure Mode check box to restrict access to Secure Web Admin and Secure Shell. This will protect administrative passwords when they are sent over the network to the appliance.

Time Synchronization

Configure Network Time Protocol (NTP) to ensure timestamps of compliance-enabled volumes are accurate. NTP synchronizes the system clock with multiple redundant servers and diverse network paths to achieve high accuracy and reliability. For information about how to set up NTP, see Chapter 4 of the *Sun StorageTek NAS OS Administration Guide*.

Related Documentation

For more information about the Sun StorageTek Compliance Archiving System, see the product documentation for your appliance at this URL:

```
http://www.sun.com/products-n-solutions/
hardware/docs/Network_Storage_Solutions/nas/
```

Title	**Part Number**
Sun StorageTek NAS OS Administration Guide	819-4284-*nn*
Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide	819-4283-*nn*
Sun StorageTek NAS OS Software Release Notes	819-6652-*nn*
Sun StorEdge 5310 NAS Appliance and Gateway System Getting Started Guide	819-3237-*nn*
Sun StorEdge 5310 NAS Appliance and Gateway System Administration Guide	819-3238-*nn*
Sun StorEdge 5210 NAS Appliance Administration Guide	819-5376-*nn*
Sun StorEdge 5210 NAS Hardware Installation, Configuration, and User Guide	817-6660-*nn*
Sun StorEdge 5210 and 5310 NAS Appliance and Gateway System Release Notes	819-2857-*nn*