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. 819-4196-13
March 2007, Revision A

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

Please
Recycle

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 any of the Sun StorageTek NAS appliances or gateway systems.

The appliance or gateway system connects directly to a network as easily as a network printer. It features high-speed RAID controller architecture and redundant components that improve data availability. The modular, scalable appliance or gateway system offers nonstop performance for optimum file-sharing capabilities.

The Sun StorageTek Compliance Archiving Software is extension software, enabled by a license key, that provides compliance with stringent data management and retention requirements. You can configure the system for mandatory or advisory enforcement:

- Mandatory enforcement fulfills strict requirements such as those of the Securities and Exchange Commission (SEC 240.17a-4)
- Advisory enforcement satisfies less stringent requirements such as a business's internal rules for document management and retention or to help comply with other regulations, for example, Sarbanes-Oxley, Basel II, HIPAA, and 21 CFR 11.

Note – Mandatory enforcement is not available for the gateway systems, Sun StorageTek 5320 NAS Gateway System or Sun StorEdge 5310 NAS Gateway System. These systems cannot enforce access to other elements of a SAN and therefore cannot guarantee the security or integrity of retained data.

With the Sun StorageTek Compliance Archiving System providing the storage component, a complete compliance solution requires a software application so that users can manage documents and records, for example, Sun Partner Advantage Program Enterprise Content Management (ECM) applications or Integrated Document Archive and Retrieval Systems (IDARS) applications.

In addition to the storage and management system, your business practices and IT policies create the complete compliance solution.

Note – Compliance archiving is not supported on iSCSI LUNs.

System Description

This section provides details of the Sun StorageTek Compliance Archiving System.

Features of the NAS Storage

The storage component of the Sun StorageTek Compliance Archiving System can consist of any of the following:

- Sun StorageTek™ 5320 NAS Appliance
- Sun StorageTek 5220 NAS Appliance
- Sun StorageTek 5320 NAS Gateway System
- Sun StorEdge™ 5310 NAS Appliance
- Sun StorEdge 5310 NAS Gateway System
- Sun StorEdge 5210 NAS Appliance.

The appliances are mid-tier, network-attached, software and hardware that provide file services to both UNIX® and Windows clients, using standard access protocols such as Network File System (NFS) and Common Internet File System (CIFS).

Each appliance and gateway system provides the features typical of network-attached storage (NAS) appliances, including point-in-time file system checkpoints ("snapshots"), and clustering for high availability.

Each appliance can be configured to use SCSI, Fibre Channel (FC), Serial Advanced Technology Attachment (SATA) disk drives, or as a Gateway system to other network storage. The storage capacity is configurable and can be scaled as needed:

- The Sun StorageTek 5320 NAS 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 StorageTek 5220 NAS Appliance can be scaled to 24 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 Software

The Compliance Archiving software operates on file volumes that have been created as compliance-enabled. Its functionality consists of these major features:

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

For test environments or for deployments with less stringent requirements, the Compliance Archiving Software provides the option of advisory enforcement that overrides some of these features.

With the standard, mandatory enforcement, no one can delete a WORM file before its retention date, decrease a WORM file's retention time, or delete a compliance volume. Under the advisory enforcement option, authorized administrator can decrease a WORM file's retention time and delete a WORM file before its retention date. These operations are logged in the audit log.

Note – File volumes that are compliance-enabled might have slightly lower performance than volumes without this protection.

WORM Files

The term “WORM” means “write-once, read-many” and indicates that the file is archived in non-rewritable, non-erasable storage. A more accurate description is to call these files “permanent read-only” files.

A file can be created with the normal access controls and modified as needed, but after it becomes a WORM file, the Compliance Archiving software enforces stronger access controls than the traditional file access semantics provided by the NFS and CIFS protocols.

When a data management application designates a file as WORM, the file becomes permanently immutable. WORM files cannot be modified, extended, or renamed. A WORM file can be deleted only when its retention time has been met and in accordance with the file retention rules.

In addition to providing storage for WORM files, the Compliance Archiving System supports backup to immutable tape media, or WORM tape.

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

File Retention Periods

The Compliance Archiving Software associates a retention period with each WORM file. If you or the data management application that writes files to the volume does not set a retention period explicitly for each file, the default retention period is used.

When the retention period expires, you can delete a WORM file or extend its retention period. With the advisory compliance option, you can decrease the retention period for a file to allow it to be deleted. With the mandatory compliance option, you cannot decrease the retention period.

Caution – If you or the data management application that writes files to the volume does not set a retention period explicitly for each file before making the file WORM, the default retention period for the volume is used. You can change the volume's default, but under mandatory compliance, this default retention period is permanent.

Administrative Lock-Down

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

Compliance Audit

The Compliance Archiving Software retains immutable records of all compliance-related activities that occur on the system. It maintains a text-based log file for attempted efforts to modify or delete data, with or without proper authority, and is enabled through the use of the Data Retention Audit Service (DRAS) API, which includes the following features:

- Accountability of changes and attempted changes to retained files
- A logging mechanism through which events that are audited are stored
- Protection and preservation of the audit log for the life of the system
- The log is in a viewable format and has secure access through standard system access protocols.

The following events are audited:

- Retention of a file
- Extension of the retention period on a retained file
- Requests to unlink (delete) a retained file

- Requests to write to a retained file
- Requests to rename a retained file
- Requests to remove a directory
- Requests to rename a directory

A full description of the audit log provided by this service is in Chapter 9 of the *Sun StorageTek NAS OS Administration Guide*.

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 and found to be infected, the file is quarantined. Quarantined files are not retained.
- If a retained file is scanned for viruses and found to be infected, access is denied.

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

Hardware Configuration Recommendations

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

Physical Security

Software features and hardware storage 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 must monitor the state of the batteries in the RAID Controller and the system BIOS and replace them in accordance with Sun's maintenance guidelines.

Back-End Storage

The Sun StorEdge 5300 RAID EU Controller Enclosure and the Sun RAID expansion unit controllers must 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. If other computers are attached to the RAID controllers, the Compliance Archiving Software can no longer protect WORM files from accidental or malicious corruption.

The only circumstance in which an expansion unit can ever be connected to a computer that is not part of the appliance is when authorized and trained Sun Service personnel are troubleshooting an appliance or gateway system.

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

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.

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 enforces data retention rules and policies so some file system operations behave differently on compliance-enabled file systems than they do on non-compliant file systems. To ensure the correct management of retained data, the Sun StorageTek Compliance Archiving Software must be used by applications that have been modified explicitly to manage file

retention, using the Sun StorageTek Compliance Archiving Software's API. This interface and the 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 is the default mode. The API for the default mode is available from Sun Microsystems and documented in Appendix C of the S*un StorageTek NAS OS Administration Guide*.
- 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 emulation
```

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 must be limited to secure protocols. To configure the appliance to limit remote access, follow the directions 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 protects 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 NAS OS Software Release Notes	819-6652-*nn*
Sun StorageTek 5320 NAS Appliance and Gateway System Getting Started Guide	819-4283-*nn*
Sun StorageTek 5220 NAS Appliance Getting Started Guide	819-7167-*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*