Contents

4 Using AUDITCON for Volume Auditing

5 Using AUDITCON for Container Auditing

6 Using AUDITCON to Audit External Audit Trails

A Audit File Formats

Trademarks

How to Use This Manual

Introduction

Auditing the Network is for administrative staff (auditors, supervisors, administrators, and operators) of NetWare® Enhanced Security servers. It is not intended for nonadministrative network users.

The purpose of this manual is to

- Show individual auditors, acting independently of network supervisors and others, how to audit network event transactions.
- Show auditors how to audit Novell Directory Services™ (NDS™) events and events specific to a volume's file system or server.

Auditing the Network, when combined with the *NetWare Enhanced Security Manual*, addresses the recommended content of the Guidelines for Writing Trusted Facility Manuals [NCSC-TG-016] but, as described in Paragraph 1.3 of that manual, presents the information in a different order and format than the recommended outline.

In Novell documentation, an asterisk denotes a trademarked name belonging to a third-party company. Novell trademarks are denoted with specific trademark symbols, such as ™.

Manual Overview

This manual contains NetWare Enhanced Security information that describes the effective use and administration of the NetWare server's audit mechanisms and the NetWare Enhanced Security AUDITCON (AUDIT CONsole) utility.

Auditing the Network replaces Chapter 8, "Auditing NetWork Events," of the NetWare 4.1 *Supervising the Network* manual. It describes procedures for

- Controlling access to audit data
- Protecting the audit utilities
- Guarding against loss of the audit configuration and audit data
- Maintaining an audit console log

Additional NetWare 4.11 documents are available online, using the DynaText* viewer (see *Installing and Using Novell Online Documentation* for information on using the DynaText viewer). Security-related documents include *NetWare Enhanced Security Administration, NetWare Enhanced Security Server,* and *Security Features User Guide.*

NetWare Enhanced Security

Enhanced Security refers to the C2 evaluated configuration for NetWare 4.11. It defines the hardware and software that can be used in a C2 server. Use of any hardware or software not listed in *NetWare Enhanced Security Server* is outside the scope of the server evaluation.

User Comments

We are continually looking for ways to make our products and our documentation as easy to use as possible.

You can help us by sharing your comments and suggestions about how our documentation could be made more useful to you and about inaccuracies or information gaps it might contain.

Submit your comments by using the User Comments form provided or by writing to us directly at the following address:

Novell, Inc.
Documentation Development PRV-C231
122 East 1700 South
Provo, UT 84606 USA
e-mail: commentdoc@novell.com

We appreciate your comments.

chapter 1

Concepts of NetWare Auditing

This chapter introduces concepts of auditing a NetWare® Enhanced Security network. These concepts are

- NetWare auditing
- Audit trail
- Audit File object
- Auditing in a client-server network
- Independent auditor

NetWare Auditing

Auditing means collecting and examining records to make sure that the server's resources are protected by the server Trusted Computing Base (TCB).

The server provides protected mechanisms to record audit information in a protected audit trail. Individuals known as auditors can then review this information or configure the server to collect other information.

For more introductory information, refer to "Auditing" in *Concepts*.

Audit Trail

An audit trail consists of

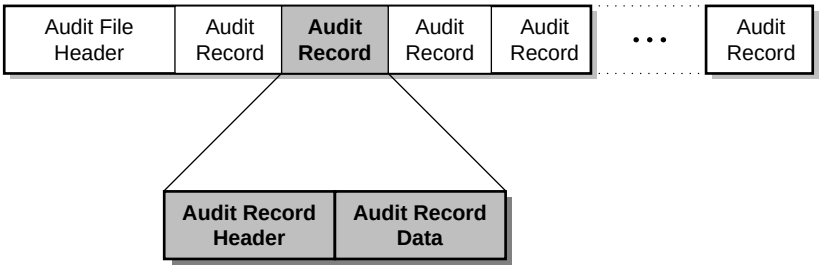
- An NDS Audit File object
- A sequence of audit data files

The Audit File object and its Novell Directory Services™ (NDS™) properties define the audit configuration and the rights of other NDS entities to access the Audit File object and its audit files. Refer to "Audit File Object" on page 5 for more information.

The sequence of audit data files include the current audit file (where data is currently being recorded), up to 15 old online audit files, and a sequence of offline audit files.

As shown in Figure 1-1, each audit file consists of an audit header followed by a sequence of audit records, where each record contains information about a specific audit event. Refer to Appendix A, "Audit File Formats," on page 267 for definitions of volume, container, and external audit file formats.

Figure 1-1
General Structure of Audit File



The complete audit trail consists of a sequence of audit records that potentially extends from the first audit event recorded on an offline audit file to the last audit event recorded on the current audit file. The audit file header includes a creation timestamp that determines the position of each audit file in the sequence.

Each audit record is timestamped with the originating server's local time. Events on different servers are synchronized by NDS time synchronization mechanisms, which usually maintain times on multiple servers to within a second of each other.

Audit records can logically be divided into two types:

- Audit history records, which record such management actions as examining or configuring the audit trail
- Audit event records, which record user actions that were audited by the NetWare server or an external client

Audit history and audit event records are physically stored together in audit data files. However, AUDITCON provides separate facilities to examine the two types of records.

Audit history records are always recorded if auditing is enabled; you cannot use preselection (advance specification of the events, users, and files to be audited) to avoid recording audit history records.

The NetWare Enhanced Security server manages the types of audit trails shown in Table 1-1.

Table 1-1
NetWare Enhanced Security Audit Trails

Volume audit trails	A volume audit trail is associated with a single volume on a single server. The audit data is stored in the volume on that server. The volume audit trail contains audit history events for the volume audit trail, plus security-relevant events recorded by the server's operating system (mount volume, for example) and file server software (file open and file deletion, for example). The audit configuration (rules for generating audit events and other items) is specified by volume, so that auditing can be enabled for one volume and disabled for another volume. Volume audit events can be preselected based on event type, user identity, and (for certain file system events) on filename. In addition to the events that can be recorded in each volume audit trail, the SYS: volume audit trail can also record events detected by the server's operating system. These include console events, such as loading NLM™ programs and defining SET parameters. Because the server does not provide a mechanism for logging in administrators at the server console, console auditing must be supported by a manual log that identifies which administrator is using the server console.

Table 1-1 *continued*
NetWare Enhanced Security Audit Trails

Container audit trails	Container audit trails record security-relevant Novell Directory Services (NDS) events performed in the associated NDS container object, as well as audit history records for the audit trail. Because NDS is a distributed database, container audit trails are associated with the distributed NDS container object and not with any specific server (as with volume audit trails). Container audit trails (but not necessarily all events in the audit trail) are replicated to each partition holding the audited container object. The audit configuration is specified separately for each audited NDS container object. Preselection of container audit events can be configured in one of two ways: event only (this is the default) or auditor by user as well as by event. Auditing of a particular container object (an Organization object, for example) does not imply auditing of subcontainers within the audited container (its Organizational Unit objects, for example).
External audit trails	The server provides external audit trails that can be used by trusted clients to store audit data on the server. External audit trails also contain audit history records. Preselection of client-generated audit records is performed by the client before submission of audit records to the server. The NetWare server sees the external audit information as a stream of un-interpreted data; interpretation of the audit events is performed solely by the client Trusted Computing Base (TCB).

Figure 1-2 shows an example of these audit trails on a two-server network. Each of the audit trails is maintained, configured, and controlled separately. Each server can have its own volume audit trail and each NDS container can have its own container audit trail.

Server 1 has eight audit trails: volumes SYS:, BETA:, and GAMMA:; containers ACME, SALES.ACME, and LAB1.ENGR.ACME; and external client audit trails EXT1 and EXT2.

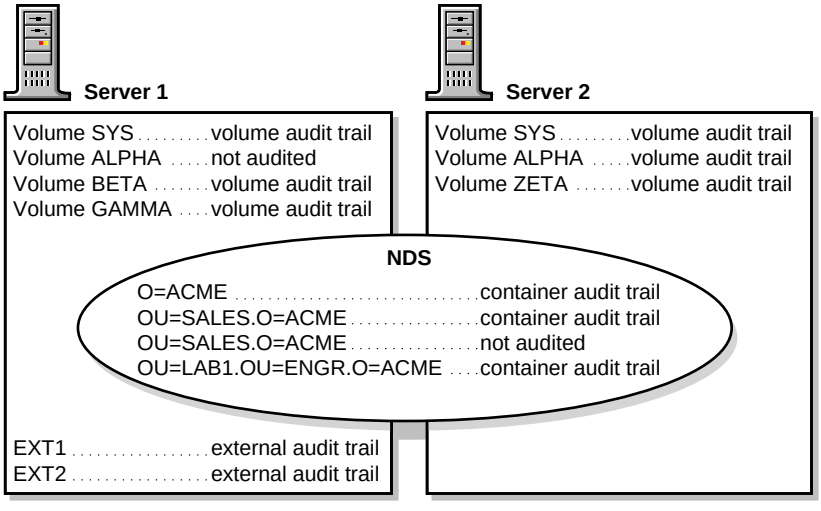
Server 2 has six audit trails; volumes SYS:, ALPHA:, and ZETA:, and containers ACME, SALES.ACME, and LAB1.ENGR.ACME.

NDS is a global network database. The description of a particular server having a container audit trail assumes that the container exists in an NDS partition that is replicated on that server.

If a container is in a partition that is found only on Server One, then Server Two would not have a copy of that container audit trail. See

Chapter 5 “Managing the Novell Directory Tree” in *Supervising the NetWork* for more information on replicating partitions.

Figure 1-2
Examples of NetWare Enhanced Security Audit Trails

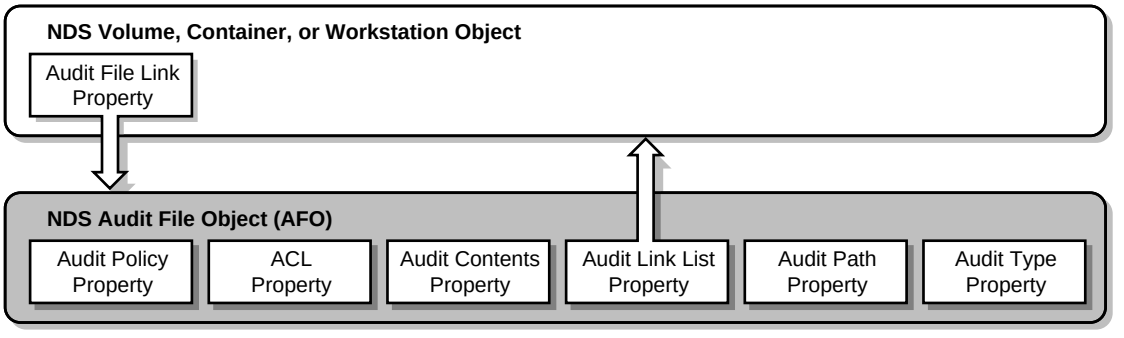


Audit File Object

The Audit File object is the NDS data structure used to manage an audit trail’s configuration and access rights. Figure 1-3 shows the important object properties of the Audit File object, and the relationship of that object to the volume, container, or clients being audited.

The Audit File object has other properties that are not shown. The Volume, container, or workstation NDS object that is audited has an Audit File Link property pointing to the Audit File object.

Figure 1-3
Audit File object



Volumes are always represented by NDS Volume objects, and containers by NDS container objects such as an Organization object or an Organizational Unit object. The type of NDS object used for representing workstation objects depends on the client software.

Table 1-2 defines the context in which your audit trails are configured and accessed. Normally, except for setting access controls, you will not need to directly manipulate the Audit File object or its properties.

Table 1-2
Audit File Object Properties

Audit Policy	The Audit Policy property stores audit configuration data for the audit trail. It includes the maximum size of the file, the number of old online audit files to be maintained by the server, a map of events to be audited, and other information. Users with the Read right to this property can read the auditing configuration. Users with the Write right to this property can modify the audit configuration and destroy old audit files.
Audit Contents	The Audit Contents property has no specific values. However, users with the Read right to this property can read the contents of any of the underlying audit data files. Subjects with the Write right to this property can append audit events to the current audit data file.
Access Control List (ACL)	Defines the rights held by other NDS objects to the Audit File object and its properties.
Audit Link List	Defines the links to the NDS Volume, container, and workstation objects that are audited in the audit trail.

Table 1-2 *continued*
Audit File Object Properties

Audit Path	For external audit trails, this property points to the volume (and, implicitly, to the server) that store the audit data files associated with the external audit trail. The Audit Path property is not necessary for volume and container audit trails; the pathnames are implicitly known for these audit trails.
Audit Type	Defines whether this Audit File object represents a Volume, container, or external audit trail. This property is used by AUDITCON when locating external audit trails.

Your audit utility (AUDITCON, for example) creates the Audit File object when you enable auditing, and the Audit File object is transparently checked by the server for access rights each time a user attempts to access the audit trail.

Auditing in a Client-Server Network

Within the NetWare client-server environment, client and server components provide cooperating audit mechanisms to support your organization's auditing policy.

The audit architecture described in this section addresses

- Information flows from user and administrator actions to protected audit trails within the server
- Means for specifying and reviewing audit configuration data
- Flows of audit information from the audit trails to a client for post-processing

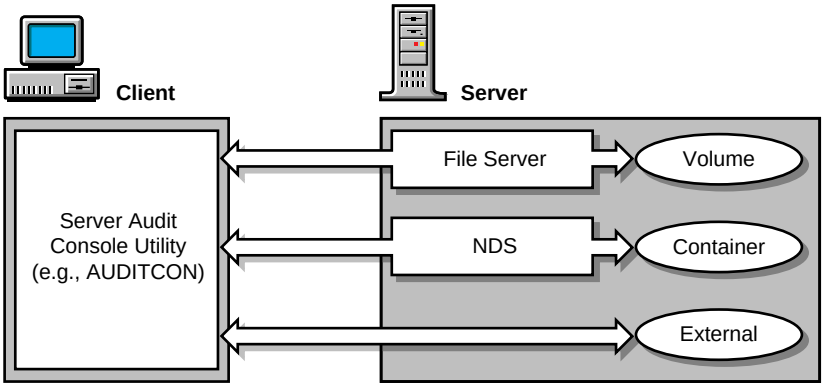
Figure 1-4 shows the architecture of the client and server software used by an auditor to configure the server's auditing mechanisms. There are no server-based utilities for this task; instead, auditors use client-based utilities (AUDITCON, for example) to enable auditing and to specify audit preselection parameters (which events, users, and files to audit).

This manual describes how to use AUDITCON. You are not required to use AUDITCON for NetWare audit administration. You can use any third-party tool in its place, as long as that tool has been included in your client workstation's Trusted Computing Base (TCB). See the

documentation provided by your client vendor to determine what tool or tools can be used for NetWare audit administration.

The server's protected software (operating system, server, and NDS) stores this information in the associated volume, container, or external audit trail. It uses the configuration information to selectively audit events that have been specified by an auditor.

Figure 1-4
Audit Configuration Interactions



As shown in Figure 1-5, protected code in the server generates audit events to audit trails protected by the server. The operating system records console commands in volume SYS: audit trail.

The server processes client file, queue, and server NetWare Core Protocol™ (NCP™) messages and, based upon the current audit configuration (preselected events, users, and files), generates audit events to the appropriate volume container.

The NDS software processes incoming NCP messages and, based on the current configuration of preselected events and users, generates audit events to the appropriate container audit trail. The server also provides a mechanism for trusted client programs to record data in an external audit trail.

Figure 1-5
Audit Generation Flow

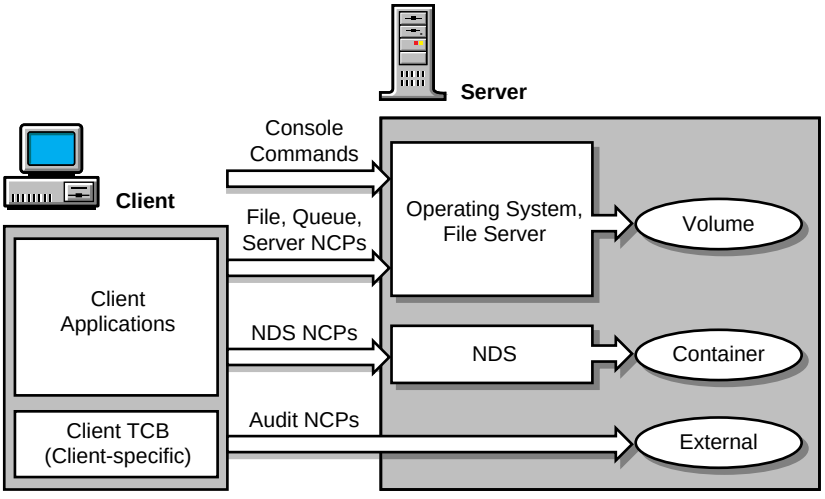
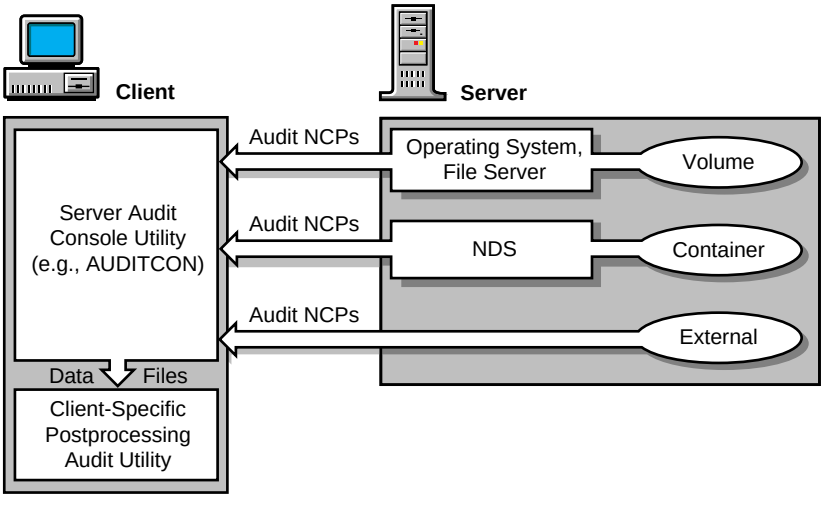


Figure 1-6 shows the architecture of the client and server software used by an auditor to perform audit processing. There are no server-based utilities for processing the server's audit trails; instead, auditors use client-based utilities (such as AUDITCON) to review audit trails and to display selected audit events.

In addition, if a client component stores its audit events in a server-provided external audit trail, the client must provide a client-specific utility for post-processing of those audit events after they are extracted from the server audit trail by AUDITCON.

Figure 1-6
Audit Post-Processing Flow



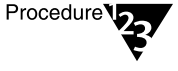
Creating the Auditor Account

For an auditor to audit the operation of a NetWare Enhanced Security server, a network administrator must first create an account for the auditor.

"User Account Administration (Client)" in *NetWare Enhanced Security Administration* describes procedures for creating user accounts in a trusted network facility. "Protecting Administrative Accounts (Client)" in *NetWare Enhanced Security Administration* describes additional requirements for protecting administrative and auditor accounts.

The following procedure describes how an administrator creates your auditor home directory, creates your auditor User object, gives your Auditor object rights to the home directory, and maps a drive on your client workstation to the audit programs on the server.

Procedure



1. **Create a directory in the file system for the auditor to use.**

   The auditor needs space to store audit reports. Consider creating a directory in SYS:HOME or wherever you have created other user account directories.

2. **Create the auditor as a User object.**

3. **If the auditor will audit NDS events, assign the auditor the Browse object right for the container objects to be audited.**

4. **Give the auditor trustee rights to the directory you created for the auditor.**

   You can grant the auditor the Supervisor trustee right to the directory, or you can assign the auditor all rights but the Supervisor right. Either method produces the same result.

5. **Map a drive to the directory containing the audit program files.**

6. **If you have not included a search drive mapping to SYS:PUBLIC in the system login script, create a user login script for the auditor and map a drive to this directory.**

7. **Give the auditor the Browse object right and the File Scan directory trustee right to SYS:PUBLIC.**

   AUDITCON and Unicode* files are in SYS:PUBLIC unless you have moved them.

Each auditor also needs rights to the Audit File objects corresponding to the audit trails he or she is responsible for managing. See “Controlling Access to Online Audit Data” on page 17 for a definition of the rights needed for audit trail management.

Optional Steps for Increased Auditor Isolation

The administrator can create the auditor User object in any container in the Directory tree. However, for increased isolation from administrative users, you might want to request the administrator to perform the following additional steps.

Procedure

1. **Create a separate NDS container to hold auditor User objects.**
2. **Create an auditor User object who has all rights to the container.**

   Subsequently, this auditor will perform all administrative functions (such as adding other auditor User objects, setting rights, and deleting auditor objects) in the auditor container.

3. **Set an Inherited Rights Filter (IRF) for the auditor container object to filter out all inherited rights.**

   This will prevent administrators (other than the auditor created in Step 2) from accessing the auditor container object.

4. **Enable auditing for the auditor container object.**

   The administrator must run AUDITCON to enable auditing. This creates the Audit File object in the tree. The administrator must then give the auditor rights to this object.

5. **Edit the ACL for the container object to remove the administrator (other than the auditor created in Step 2) as a trustee of the container.**

6. **Edit the ACL for the Audit File object associated with the container to remove the administrator (other than the auditor created in Step 2) as a trustee of the Audit File object.**

These steps help isolate auditor accounts from non-auditor administrative users, but do not protect auditor data from administrative users.

Overview of Auditor Responsibilities

An auditor is an individual who is authorized by an organization to use the network's auditing mechanisms to identify attempted or successful access by users to unauthorized information. The educated use of the server's auditing mechanisms by one or more trusted auditors is essential to ensure the principle of individual accountability (to determine who did what and when the event occurred). The auditor's responsibilities include the following general tasks:

- Enabling and configuring auditing.
- Ensuring that audit programs, control data, and audit trails are properly protected.
- Monitoring of the server volumes and audit data files to ensure that there is sufficient space for collection of audit data. The auditor is responsible for archiving and removing audit files when necessary to prevent automatic shutdown when audit files or disk space is exhausted.
- Reviewing audit data to find attempts to circumvent the security of the network.
- Reviewing the sufficiency of audit data being collected.
- Backing up the current audit configuration, including keeping a manual log for any information that is not handled by backup and restore utilities.
- Managing offline audit files backed up on removable media.

Specific procedures are described subsequently for the auditor to accomplish these general tasks.

Independent Auditor

The server was developed to support the notion of an independent auditor. In general, except for creating the auditor's account and setting up the auditor's access rights, the actions of the auditor don't depend on the actions of administrators.

However, the notion of the independent auditor is not absolute. By running unevaluated NLMs, which is prohibited in *NetWare Enhanced Security Administration*, administrators can modify NDS to prevent auditors from performing auditing.

In addition, administrators can subvert an auditor's intended volume audit configuration by backing up a file system and then restoring it, which deletes all audit configuration information about the volume.

Thus, the independent auditor is not a completely independent role in the sense specified in the *Trusted Computer System Evaluation Criteria* (DoD5200.28-STD). In the evaluated configuration, it is not necessary to have an auditor separate from the administrator. Nonetheless, the ability to separate auditor and administrator activities is useful in most organizations.

Independent Control of Different Audit Trails

Because the server records audit information in separate container and volume audit files, audit responsibilities can be allocated to multiple auditors so that each auditor has responsibility for one or more audit trails.

Dividing auditing responsibilities works very well for auditing NDS containers. Container objects are commonly set up to reflect the structure of an organization. For example, in Figure 1-2 on page 5, each container object can be separately audited by a different auditor.

Thus, a member of the sales organization can audit the Organizational Unit OU=SALES.O=ACME, while a member of the engineering organization can audit the OU=ENGR.O=ACME container. Similarly, the organization responsible for each server can assign an independent auditor for the individual volume audit trails on that server.

The division of auditing responsibilities among multiple, isolated auditors means that an individual auditor will not have access to supporting audit information in

other audit trails. For example, if you are the auditor of the SYS: volume audit trail, but do not have access to other container and volume audit trails, you cannot track a user's activities throughout NDS and other volumes. To audit the overall network system, as required for a NetWare Enhanced Security system, at least one auditor must have rights to all audit trails.

The existing AUDITCON utility described in this section does not provide a means for correlating multiple volume and container audit trails, or for correlating the servers' audit trails with clients' external audit trails. Correlation of multiple audit trails must be performed manually. One way is to generate individual printed audit reports for each desired volume or container, and then merge or sort the various reports into a single trail.

Overview of Surveillance Methods

Trusted NetWare provides two general methods of performing surveillance of users' accesses to protected resources.

- **Post-processing** is a method of filtering an existing audit trail to present only the events that are of interest. AUDITCON provides menus to define post-processing filters for volume, container, and external auditing.

- **Preselection** is a method of causing the server to record selected event types (such as file opens), specific users, or specific resources (such as files or directories) to the current volume trail. For volume auditing, you can preselect by event types, users, and files.

  For container auditing, you can preselect by users and event types. The server does not provide any preselection for external auditing. For preselection of external auditing, see your client documentation.

You cannot generate audit reports for events that are not preselected for auditing when the event occurs. For example, if you want to review which files were opened by a user two weeks ago, but you did not have file opens preselected at that time, you will not be able to generate an audit report that lists the files. Consequently, you must balance your need for certain audit information with the resources required to audit those events.

chapter 2

Protecting Audit Data

The server provides a protected environment that generates and records audit data. However, to provide continuous audit coverage, you must ensure that audit configuration data, collected audit data, and audit programs are properly protected. This is accomplished by

- Controlling access to the online audit data
- Protecting audit utilities
- Protecting audit data on removable media
- Backing up the audit configuration
- Preventing loss of audit data
- Backing up audit data
- Maintaining a console audit log

Controlling Access to Online Audit Data

The server provides two separate methods for controlling access to online audit configuration data and recorded audit files:

1. NDS™ provides an Audit File object for each audit trail that defines the access rights to the audit configuration and audit data. “Audit File Object” on page 5 describes the NDS object property rights that mediate access to the audit trail. The server checks the Audit File object’s NDS rights when you try to access an audit trail or make changes to the Audit File object properties. If this check succeeds, the user can access the audit trail. This is the only approach that is permitted for NetWare Enhanced Security servers.

2. For compatibility with previous NetWare® releases, the NetWare Enhanced Security server also supports an optional password-based access control method. This option is enabled on individual servers by setting the ALLOW AUDIT PASSWORDS console parameter. If audit passwords are enabled at the server console, the single-level audit password controls access to all aspects of the audit trail.

   You can also configure the audit file to use dual-level passwords, where the first level password is required to view the audit data and the audit configuration, and the second level password is required to change the audit configuration.

The default value for ALLOW AUDIT PASSWORDS is OFF, meaning that access to the audit data is controlled solely by the Audit File object's object property rights.

However, in systems that do not comply with the NetWare Enhanced Security configuration, administrators can configure servers to permit the use of audit passwords. Such configuration is done on a server-by-server basis, so that mixed configurations are possible—some servers using the Audit File object rights-based access controls and other servers using audit passwords.

The server's NetWare Enhanced Security configuration requires use of the Audit File object rights-based access control mechanism to protect audit data. Do *not* enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON), because this violates the assumptions under which the server was evaluated.

When an audit utility (AUDITCON, for example) creates an Audit File object, the server gives the creator the following rights:

- The Supervisor right [Entry Rights] to the Audit File object
- The Write right to the Access Control List property

AUDITCON also assigns additional rights. The following rights are assigned to the creator of the Audit File object:

- Read and Write rights to the Audit Policy property
- The Read right to the Audit Contents property

These rights allow the auditor who created the Audit File object to read audit files, change the audit configuration data, and assign access rights to other auditors. If you are working in a single-auditor environment, this might be sufficient for your needs. You (or any other user with the Write rights to the Audit File object Access Control List property) can use NETADMIN, NetWare Administrator (NWADMIN), or other utilities to define rights for other auditors.

See your client documentation for information on the availability of NetWare Administrator NETADMIN in your client evaluated configuration.

You can have three logical groupings of rights. (These rights groupings are conceptual; you can organize rights any way you find convenient.)

- Audit Viewers (who are responsible for reviewing audit trails, looking for anomalies, and generating reports)
- Audit Administrators (who are responsible for the tasks of Audit Viewers and are also responsible for configuring the audit subsystem and performing audit data backup and recovery)
- Audit Sources (which are client NTCB partitions that append audit records to server audit trails)

Table 2-1 shows the rights required for each of these three groups.

Table 2-1
Auditor Access Profiles

Auditor Access Profile	NDS-Based Access	Password-Based Access
Audit Viewer	R to Audit File object Audit Policy	Level 1 password
	R to Audit File object Audit Contents	
Audit Administrator	R to Audit File object Audit Policy	Level 2 password
	W to Audit File object Audit Policy	
	R to Audit File object Audit Contents	
Audit Source (a specific volume, container, or external source)	W to Audit File object Audit Contents	N/A
	R to Audit File object Audit Path	

The server checks whether you have the appropriate rights when performing each action and refuses to perform the action if you don't

have those rights. If you revoke access rights to an auditor who is already accessing an audit file, these changes do not take effect until the auditor tries to reestablish access to the volume or container audit trail.

AUDITCON doesn't modify rights to the Access Control List property. You can use other utilities (NETADMIN or NetWare Administrator) to assign other users rights to the Access Control List property.

See your client documentation for information on the availability of NetWare Administrator or NETADMIN and in your client evaluated configuration.

Do not give untrusted users (individuals who are not auditors or administrators) any rights to the Audit File object (or its properties) except the Browse right.

There is more than one way to establish these rights. You could create several Organizational Role objects for each grouping of related audit trails.

For example, you might have an object called "Engineering Partition Audit Viewer" that would be a trustee with the Read right to the Audit Policy and Audit Contents properties of the Audit File object associated with each container in the "Engineering" partition.

Another object called "Engineering Partition Audit Administrator" could be a trustee with the Read and Write rights to the Audit Policy and Audit Contents properties of the Audit File object for each of the same containers.

Individual administrators could then be made security equivalent to whichever Organizational Role object is appropriate for their responsibilities. Alternately, individual users could be made trustees of those Audit File objects that they are responsible for managing.

There is no requirement to divide up the rights to audit files. In some organizations, a group of administrators has the authority to manage all aspects of the organization, including audit management. In this case, all individuals in that group might have the Supervisor right to the root of the Directory tree, with no Inherited Rights Filters to block rights. In this scenario, there is no need to directly assign rights to properties of an Audit File object, since the administrators will gain those rights through inheritance.

The server does not provide any locking mechanism to prevent multiple auditors from simultaneously attempting to change volume, container, or external audit

configuration data. If this occurs, the last auditor to write the audit configuration might overwrite changes made by other auditors. If you have more than one auditor who has rights to modify the audit configuration, you must institute procedural methods to control access to the Audit File object, such as selecting a single replica of the Audit File object and making all changes to that replica.

Protecting Audit Utilities

AUDITCON is stored in SYS:PUBLIC of the server file system, from where it is normally executed by the client workstation. Because AUDITCON runs with your identity and has your rights to the audit trails you manage, it is essential that AUDITCON be write-protected to prevent modification by untrusted users.

Permanently loading AUDITCON on your local trusted workstation is not recommended. Loading it locally has no advantages, and it complicates maintenance of the server Trusted Computing Base.

The audit utilities that configure and access their server's external audit trails must also be protected from modification by untrusted users. See your client documentation for information on the client-specific utilities and how they are protected.

Protecting Audit Data on Removable Media

AUDITCON provides a mechanism for backing up old volume and container audit files to removable media (diskette, tape, and so forth) and then deleting those files from the server to free up audit space.

Procedures for backing up audit files are given in Chapter 4, "Using AUDITCON for Volume Auditing," Chapter 5, "Using AUDITCON for Container Auditing," and Chapter 6, "Using AUDITCON to Audit External Audit Trails." However, once the file is copied from the server's protected file system to removable media, you must use other means to ensure that the Trusted Computing Base audit data is not compromised. Table 2-2 shows the two methods available:

Table 2-2
Protecting Audit Data

Physical protection of removable media	You must physically protect the removable media that contain the offline files to ensure that unauthorized users (anyone except an auditor) do not read or modify the audit data. When you no longer need an offline audit file, either overwrite the data on the removable media or destroy the media itself. Do not place media containing audit files back in rotation for use by other users.
Protection of offline data	When you use AUDITCON to create an offline audit data file, the offline audit data file contains an indicator of what the corresponding Audit File object was. When you use AUDITCON to process that offline audit data file, AUDITCON examines the Audit File object and determines whether you still have sufficient rights to see the data. If you don't, you won't be able to see the contents of the offline audit data file. **Note:** This protection mechanism does not replace physical protection as the primary means of protecting offline audit data. An individual who obtains the offline audit data might disable the check performed by AUDITCON or use another utility which does not perform this check. You must not rely on this mechanism to protect your offline audit data.

Backing up the Audit Configuration

To provide continuous audit protection, you must ensure that a copy of your current audit configuration is available and can be reinstalled if the online audit configuration is lost. This involves a combination of automatic mechanisms, backup software, and manual procedures.

The Audit Policy property of the Audit File object contains all of the audit configuration data for container audit trails, much of the audit configuration data for volume audit trails, and all of the audit configuration data held by the server about external audit trails.

This includes the audit file size rollover options, and a map of audited volume and container events. Because the Audit File object is an NDS object, it is automatically replicated to storage on other servers when you create or modify the Audit File object.

The Audit File object for an external audit trail does not contain client-specific information, such as what audit events are preselected by the client Network Trusted Computing Base.

In addition, you can run SBACKUP to back up the Audit File object and its properties. Refer to “Backing Up and Restoring Data” in *Supervising the Network* for more information about backing up NDS. NDS backups are intended only for recovery from catastrophic losses of NDS; the primary backup mechanism is the replication of the NDS database onto multiple servers.

SBACKUP and its Target Service Agents (TSAs) do not back up volume and container audit files. If you want to recover audit files after a server crash, you must manually back up audit files using AUDITCON or another utility.

SBACKUP and its TSAs do not back up audit preselection flags for files, directories, or users. If you audit specific files/directories or users, you must manually log that audit configuration. Otherwise, you won't be able to restore the desired audit configuration after recovering from a backup.

Preventing Loss of Audit Data

The server protects audit files to prevent unauthorized users from accessing or deleting the files. However, hardware problems, software problems, or power failures can cause the loss of audit data records or entire audit data files.

1. Individual audit records are maintained in the server's file system cache until the server writes the cache to disk. The server does not expedite the handling of audit data. The amount of audit data that can potentially be lost after a power failure is limited only by the size of the cache. To reduce the amount of audit data that can be lost, you can set the Dirty Disk Cache Delay Time to its minimum value (0.1 seconds). See “SET” in *Utilities Reference* for more information.

2. Container auditing uses the Transaction Tracking System™ (TTS™) to ensure that each audit record is separately tracked. If the server crashes, your container audit files will be on a clean audit record boundary after the crash. Volume auditing does not use TTS, so a server crash could cause part of the audit file to be corrupted. Records added after the crash will still be accessible; however, there might be partial records in the middle of the file. In such a case, AUDITCON is generally able to find lost audit records.

Improper shutdown of the server is a potential cause of file corruption (including audit file corruption). Be sure to properly down the server, then exit from the server, before turning off the server's power.

In addition to audit loss that can be caused by hardware or software problems or loss of power to the machine, you can lose audit events if the configured number of audit files are filled or disk space fills up and the audit trail is improperly configured. The server provides the following three configuration options for handling audit overflow.

- **Archive the current audit file.** When an audit file reaches its maximum size or the server is unable to write an audit record (for example, the disk is full), the server archives the current audit file. This consists of saving the current audit file as an old audit file and creating a new current audit file.

  The server can maintain online storage for up to 15 old audit files, where the maximum number of old audit files is a configuration setting of the Audit File object's Audit Policy. If the server already has the maximum number of old online audit files, it deletes the oldest of the old audit files. Use of this option is not recommended in the Enhanced Security configuration, as it can lead to data loss.

- **Continue without auditing.** Actions which would otherwise be audited are not audited by the server. Use of this option is not recommended in the Enhanced Security configuration, except in emergency situations, as it results in the loss of audit coverage.

- **Disallow audited/auditable events.** If the audit trail is a volume audit trail, then any facility which is potentially auditable (such as NCP service) is disallowed, even if that particular event wouldn't cause an audit record to be generated. If the audit trail is a container audit trail, then any event which requires auditing is disallowed, but only if that particular event would cause an audit record to be generated. If the audit trail is an external audit trail, then submission of audit records is disallowed (that is, external audit records are rejected).

  This is the only option recommended for the Enhanced Security configuration.

"Audit Trail Overflow" on page 133, "Audit Trail Overflow" on page 215, and "Audit Trail Overflow" on page 261 provide more

information on how to recover from audit overflow for volume, container, and external audit trails, respectively.

As the server approaches the configured file size limit for an audit file, it sends warnings to the server console. When the server detects a full condition in any audit file (volume, container, or external) and the selected option for that audit trail is to disallow audited / auditable events or to continue without auditing, it sends a warning to the server console and to any logged-in auditor of the audit trail.

At this point, the auditor must resolve the full condition by backing up and deleting old audit files (or ordinary files, if the situation was caused because the volume is full) and performing a manual archive, which causes the current audit file to become an old audit file, and starts a new current audit file.

When you see a message indicating that an audit trail is full, you should take immediate action to resolve the condition. Until you do, audit data will be lost (if the “continue without auditing” option is in use) or users will be unable to use the server (if the “disallow audited/auditable events” option is in use).

Backing up Audit Data

Your organization should have an audit data maintenance policy. The policy should answer these questions:

- How often should audit data be backed up in case of a disk crash or similar malfunction (since audit data is not backed up with volume or NDS data using SBACKUP)?
- Is online audit data sufficient, or do you need to back up the audit data to offline storage for long-term access?
- How long should offline audit data be stored?
- How should offline audit data be stored? Can it be kept in server files, and be backed up with other files? Or should it be stored on a client workstation or removable media?
- Is it sufficient to back up one copy of each container audit file, or do you need to back up all copies to ensure that you have a complete audit trail? (Container audit records are copied to all

servers that hold a replica of the container, but there is no guarantee that every record will be stored in all copies.)

Depending on the policies set by your organization, you might need to back up old audit files before online audit files are overwritten or deleted.

Maintaining a Console Audit Log

Actions performed at a server console can be audited, if you preselect them using volume auditing. However, the audit records will not contain any indication of who performed the action, because there is no console sign-on procedure. For this reason, you must maintain a manual log of all administrators who use the server console.

This log is used with the automated audit trail for establishing accountability for actions taken at the server console. Table 2-3 shows a sample format for a manual console log.

If you have more than one server in your network, you can keep a single log for all servers, or a separate log for each server, but make sure that administrators identify in the log which server consoles they use. If administrators do not maintain manual logs, actions taken at the server console cannot be identified with an individual.

Table 2-3
Sample Format for Console Audit Log

Date	Time On	Time Off	Server User	User
23 Mar 96	10:35am	11:22am	SERVER1	Joe Smith
23 Mar 96	10:52am	11:20am	SERVER2	Joe Smith
23 Mar 96	2:45pm	4:50pm	SERVER1	Jane Jones

Additional Cautions

Auditors can preselect individual users as having their volume and container actions audited. For details about preselecting individuals for volume and container auditing, see “Audit by User” on page 67, “User Restriction” on page 84, “Audit by User” on page 161, and “User Restriction” on page 170. The ability to preselect users is not related to the auditor’s NDS rights to the User objects.

A user who is configured as an Audit Administrator (with at least Read and Write rights to the Audit Policy property) of the Audit File object for any volume or container can preselect any user in the Directory tree.

That is, if SMITH is an auditor for volume SYS: on Server 1, then she can preselect (mark or unmark) any user in the Directory tree to be audited, even if the user being preselected is not a user of Server 1 and the User object is not in an partition stored on Server 1.

For this reason, it is important to ensure that all auditors are properly trained regarding the organization’s policy on which users are preselected.

A user who has the Write right to the Audit Path property of an Audit File object used for external auditing can redirect audit data to an alternate volume or server, thus causing loss of access to the old audit data. To do this, a user does not need any rights to the server or volume that will hold the new audit data.

The disk space taken by external audit files cannot be recovered except by a user with the Write right to the Audit Policy of the corresponding Audit File object. For example, if user SMITH is an auditor of some external audit trail A, then user SMITH can cause external audit data to be stored on all servers in the network, even if she has no rights to files on any of those servers.

Therefore, it is important to ensure that all auditors are properly trained regarding the organization’s policy on where external audit data files are stored.

chapter 3

Using the AUDITCON Utility

AUDITCON is a client utility for DOS and OS/2* workstations that allows an auditor to configure and review the server's volume and container audit trails. This chapter presents the prerequisites and procedures for running AUDITCON.

General Prerequisites

- ❑ A trusted workstation running DOS 3.30 or later.
- ❑ Sufficient memory on the workstation to run the AUDITCON utility.
- ❑ Read file rights on the AUDITCON utility and help files in the server's file system's public directory.
- ❑ NDS™ access rights or the correct audit password. Anyone can run the AUDITCON utility. However, to see audit data or to configure the auditing system, you must pass the access controls on the audit trails, either by having NDS access rights or by having the correct audit password. See "Controlling Access to Online Audit Data" on page 17.

See your client documentation for information on the availability of AUDITCON in your client evaluated configuration. Because auditors have access to the trusted computing base's audit data, you must run AUDITCON only on a trusted (C2 evaluated) workstation.

When generating reports to the screen or formatting reports in files, AUDITCON creates temporary files in your current directory. For this reason, you should run AUDITCON only from a directory that is protected from access by unauthorized users.

The term *current directory* is used in this chapter to indicate the drive and directory you were using when you started AUDITCON, whether that directory is on a client or server.

Procedure

Procedure

1. **Log in to the network.**

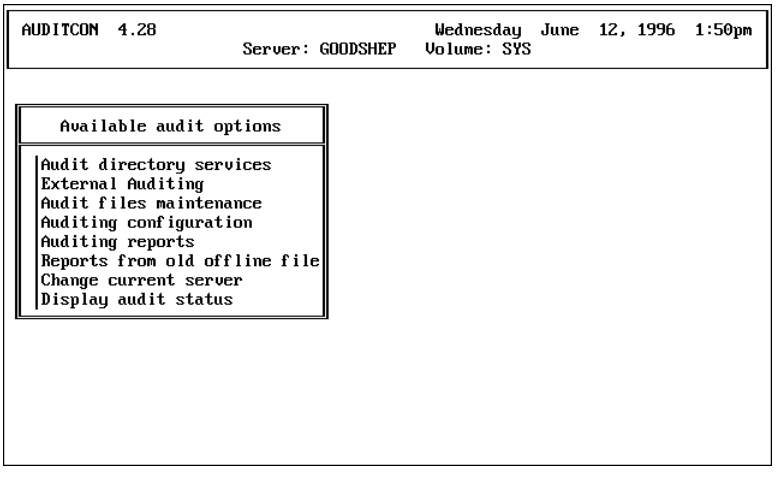
   With Novell Directory Services™, you log in once to NDS and are background authenticated to individual servers.

2. **Run AUDITCON from a network drive (for example, Z:), a local drive (for example, C:), or in your current directory, as follows:**

   `Z:\PUBLIC\AUDITCON` Enter
   `C:\AUDITDIR\AUDITCON` Enter
   `AUDITCON` Enter

   AUDITCON displays the screen shown in Figure 3-1. The screen includes a header, a menu area, and a footer line.

Figure 3-1
Initial Layout of Auditcon Screen



The two header lines shows the version of AUDITCON that you are running, the current date and time, and the current server and volume assigned by AUDITCON for your auditing session.

If you want to audit a different volume than the one shown, see “Choosing an Alternate Volume” on page 40. For container auditing, see Chapter 5, “Using AUDITCON for Container

Auditing," on page 139. For external auditing, the current server and volume information is replaced with the current NDS container context. For more information, see Chapter 6, "Using AUDITCON to Audit External Audit Trails," on page 221.

The date and time displayed in the top line of the header area are the workstation's local date and time. To make reasonable decisions about the server's audit configuration, you must ensure that your workstation Network Trusted Computing Base (NTCB) partition is synchronized with the network time maintained by NDS.

The menu area contains menus, with the most recent menu layered on top of previous menus. Menus have a header (in this example, "Available audit options", a list of available options, and a scroll bar). Use the Up- and Down-arrow keys to highlight the desired selection. If the menu has more entries than can be displayed in the menu box, the menu will show an up arrow or down arrow to indicate that there are additional choices at the top or bottom of the menu.

The footer line describes the actions associated with various keys for the current menu. For the previous example, pressing Esc exits AUDITCON, while pressing Enter selects the highlighted entry and moves to the corresponding screen in the menu tree.

3. Move down the menu tree by highlighting an entry in the current menu, choosing that entry, and finding the desired entry in the succeeding menu.

AUDITCON provides separate menu trees for volume, container, and external auditing. See Chapter 4, "Using AUDITCON for Volume Auditing", Chapter 5,"Using AUDITCON for Container Auditing", and Chapter 6, "Using AUDITCON to Audit External Audit Trails."

You can perform volume, container, and external auditing in a single session (without restarting AUDITCON), but AUDITCON does not provide any way of merging audit data or reports from multiple volumes, containers, or external audit trails.

In general, you can move back up the menu tree by pressing until you reach the top of the tree. At any time, you can press F1 for context-sensitive help.

4. **When you are finished with AUDITCON, press** Escape **until you reach the "Exit?" menu, choose "Yes" (by pressing the arrow keys to move the cursor), and press** Enter**.**

Chapter 4, "Using AUDITCON for Volume Auditing," on page 33 describes the use of AUDITCON for auditing server volumes. This includes accesses to files and directories, server events (including server console commands), and QMS events.

Chapter 5, "Using AUDITCON for Container Auditing," on page 139, describes the use of AUDITCON for auditing NDS container events.

Chapter 6, "Using AUDITCON to Audit External Audit Trails," on page 221, describes the use of AUDITCON for auditing external clients.

At any time when you are logged in to a NetWare server as an auditor, you might see a message on the workstation screen indicating that the volume, container, or external audit trail is full, and that your actions are no longer being audited. If this occurs, you must record your actions manually with respect to the volume, container, or external audit trail for use when generating a complete historical reference of actions performed on the server.

This manual recording of events performed at a client is not the same as manual recording of server console usage.

Each of the remaining chapters in this manual applies to the appropriate branch of the AUDITCON menu tree. Menu numbers, "100" for example, are not part of the displayed menu, but are used in this manual to identify specific menus. The number to the right of each menu option indicates the number of the menu that is displayed if that option is selected.

chapter 4

Using AUDITCON for Volume Auditing

A NetWare® Enhanced Security network typically has multiple servers, and each server can have multiple volumes (see *NetWare Enhanced Security Server* for more information).

Each physical volume in the network is represented by a Volume object in the Directory tree. You can use several NetWare utilities (including AUDITCON) to search the tree for Volume objects.

Although the Volume object is listed in the global Directory tree, the volume resources are associated with the specific server that manages that volume. To audit a volume, you must

- Identify the server the volume resides on
- Log in or authenticate to that server (if you have a drive mapped to the volume you want to audit, you are already authenticated to the server)

As described in "Controlling Access to Online Audit Data" on page 17, the server provides two mechanisms for controlling access to audit trails:

- Assigning NDS™ rights on the Audit File object and its object properties
- Assigning a password to the audit trail after selecting an audit configuration

  Even though the password-based mechanism is not permitted in NetWare Enhanced Security configurations, it is still used by the server and, consequently, is described in this section.

The following topics are explained in this chapter.

Accessing a Volume Audit Trail

This section describes AUDITCON's top-level menus, how to select a different current server and volume, and how to log in to a volume audit trail (if audit passwords are enabled).

If you are an auditor for multiple volumes, you perform activities on one audit trail, then return to the top-level menu and select a different volume for auditing.

AUDITCON selects a current server and current volume when it starts, based on where it was run. Consequently, you might need to change the server or the volume before you can begin auditing the volume you are interested in.

Top-Level Menus

When you run AUDITCON, it displays a screen with an "Available audit options" menu as shown in Figure 3-1 on page 30. There are five such top-level menus. The one AUDITCON displays depends on four variables:

- Whether the "Allow Audit Passwords" console parameter is set to OFF or ON. It must be set to OFF in the NetWare Enhanced Security configuration.

- Whether you have sufficient rights, defined as either
  - An Audit File object exists for the selected volume, and you have at least Read or Write rights to the Audit Contents or Audit Policy property of the Audit File object
  - An Audit File object does not exist for the selected volume, but you have sufficient rights to create an Audit File object in the container where the Volume object is stored
- Whether auditing is enabled for the volume
- Whether the volume is in the overflow state

Because AUDITCON selects a current server and volume when it starts, you might see different top-level menus based upon the initial current server and volume.

The following table summarizes the algorithm AUDITCON uses to determine which menu it displays, based on the above variables. Entries shown in italics will not occur in the NetWare Enhanced Security configuration.

Table 4-1
AUDITCON Top-Level Menu Selection

Allow Audit Passwords = ON	Sufficient Rights	Volume Audit Enabled	Volume in Overflow State	Menu
Yes	*Yes*	*Yes*	*No*	*101*
Yes	*Yes*	*No*	*No*	*102*
Yes	*Yes*	*Yes*	*No*	*103*
Yes	*Yes*	*No*	*No*	*102*
No	Yes	Yes	No	101
No	Yes	No	No	102
No	No	Yes	No	104
No	No	No	No	104

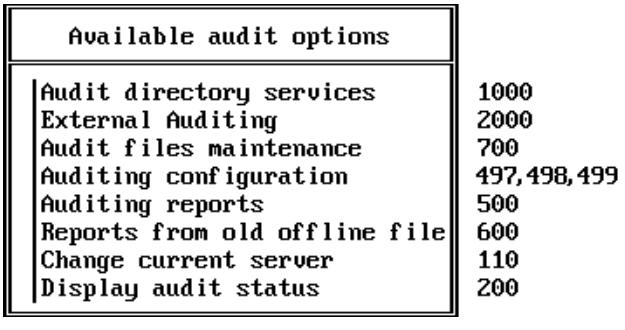
Table 4-1 *continued*
AUDITCON Top-Level Menu Selection

Allow Audit Passwords = ON	Sufficient Rights	Volume Audit Enabled	Volume in Overflow State	Menu
Yes	*Yes*	*Yes*	*Yes*	*101A*
Yes	*Yes*	*No*	*Yes*	*102*
Yes	*No*	*Yes*	*Yes*	*104*
Yes	*No*	*No*	*Yes*	*102*
No	Yes	Yes	Yes	101A
No	Yes	No	Yes	102
No	No	Yes	Yes	104
No	No	No	Yes	104

The five top-level "Available audit options" menus are described, as follows:

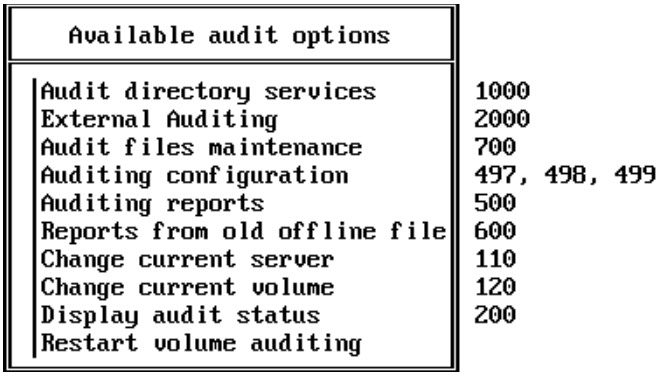
Menu 101. AUDITCON displays this menu when the auditor has rights through NDS to access the selected volume audit trail or has successfully logged in to the audit trail (when not using the NetWare Enhanced Security configuration).

Figure 4-1
Menu 101: Available Audit Options



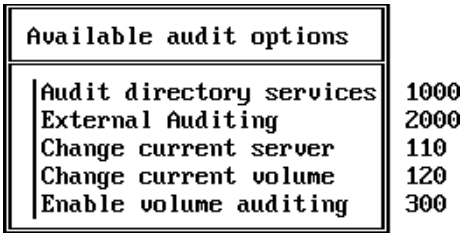
Menu 101A. This menu is similar to menu 101 but includes a "restart" option and is displayed when the volume audit trail is in the overflow state.

Figure 4-2
Menu 101A: Available Audit Options



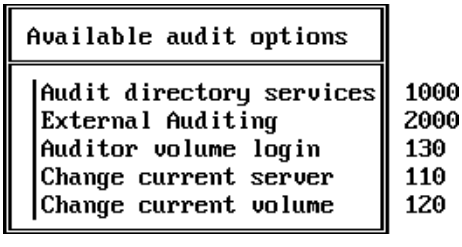
Menu 102. AUDITCON displays this menu when the current volume on the current server is not enabled for auditing.

Figure 4-3
Menu 102: Available Audit Options



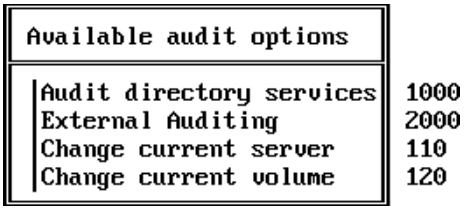
Menu 103. AUDITCON displays this menu when the current volume is enabled for auditing, but you do not have rights to read or enable the current volume audit trail. This menu does not occur in the NetWare Enhanced Security configuration because it applies only when ALLOW AUDIT PASSWORDS is set to ON.

Figure 4-4
Menu 103: Available Audit Options



Menu 104. AUDITCON displays this menu when you do not have sufficient rights to determine the state of auditing on the currently selected volume.

Figure 4-5
Menu 104: Available Audit Options



Selecting an Alternate Server

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.

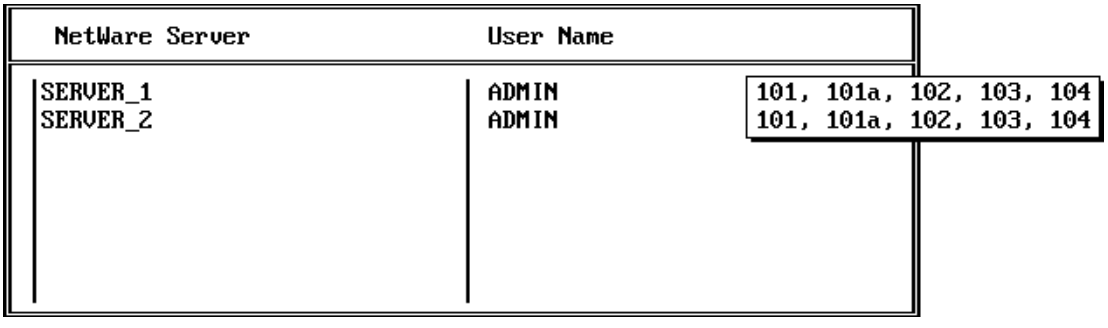
Procedure

Procedure

1. **From menus 101, 101A, 102, 103, or 104, choose “Change current server” and press** Enter**.**

   AUDITCON displays menu 110, which lists servers where you are authenticated, and your identity on each server.

Figure 4-6
Menu 110: Server List



If you are using the standard background authentication, then your identity will be the same on all servers. This menu allows you to choose a different server for auditing.

2. **Choose a different server and press** Enter**.**

   AUDITCON updates the server name in the second line of the header and returns to the previous menu.

Depending on the volume chosen on the new server, AUDITCON will display menu 101, 101A, 102, 103, or 104 (using the same rules that were used to select an initial menu).

3. **If you are using password-based access, you can press** Insert **to display a list of other NetWare servers or press** Delete **to log out from any server except the default server. Press** F3 **to change your user identity.**

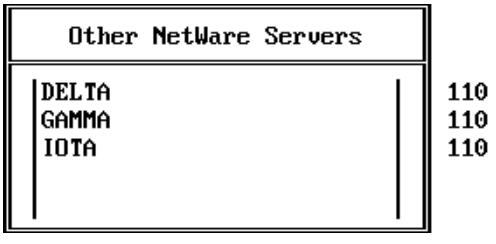
   AUDITCON displays menu 111, which provides a list of additional servers.

Note

Logging in or out of servers using this mechanism will not work in the NetWare Enhanced Security configuration. If the server you want to audit does not appear in the list in menu 110, exit AUDITCON, map a drive to a volume on the server (using the MAP command), and restart AUDITCON.

4. **Choose a server and press** Enter **to add the server to the list in menu 110.**

Figure 4-7
Menu 111: Other NetWare Servers



This list shows those servers that you are neither logged in nor background authenticated to.

5. **(Optional) If you pressed** F3 **in Step 3, AUDITCON permits you to change your user identity on the server.**

   If more than one server is listed in menu 110, AUDITCON does a bindery login (NetWare 3.x) for the name that you specify in this menu. (This is different from logging in to an audit trail; in this case, the auditor is actually changing your identity on the specified server. This identity persists after you exit from AUDITCON.)

6. **Enter the password necessary to change your identity on the specified server.**

AUDITCON requests your password for a bindery login to the server. AUDITCON does not echo your password to the screen.

If you use this method to log in to a server, you can log in only as a user whose User object is in the default bindery context. If your user ID is not in the default bindery context for the server you want to use, you should exit AUDITCON, map a drive from the server you want to access, and restart AUDITCON.

Choosing an Alternate Volume

Prerequisites

❑ See the “General Prerequisites” on page 29.

Procedure

1. **From menu 101, 101A, 102, 103, or 104, choose “Change current volume” and press** Enter**.**

   AUDITCON displays menu 120.

2. **Use menu 120 to choose a different volume audit trail on the server.**

   When you choose the new volume, AUDITCON updates the volume in the second line of the AUDITCON header.

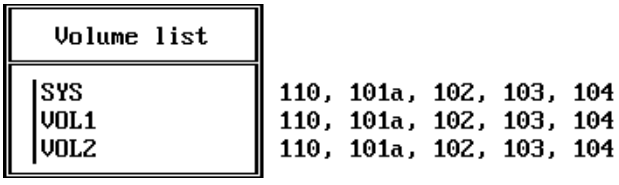
If you can't access the volume you want, exit AUDITCON, map a drive to that volume, and try again.

If the volume is enabled for auditing and you have access to the volume, AUDITCON displays menu 101 or 101A (depending on whether the volume is in the overflow state).

If the volume is not enabled for auditing, AUDITCON displays menu 102.

If the volume is enabled for auditing but you do not have access, AUDITCON displays menu 103 or 104, depending on whether password-based access is allowed.

Figure 4-8
Menu 120: Volume List



Logging in to a Volume Audit Trail

Logging in to an audit trail is different from logging in to a Trusted NetWare server. When you log in to a Trusted NetWare server, your login password is used to authenticate your identity to NDS during your login session. "Logging in" to a volume audit trail is a means of controlling access to the audit file, and is not permitted in evaluated NetWare Enhanced Security configuration.

If you decide to use audit passwords to control access to the audit trail, do not reuse your NetWare login password.

Prerequisites

Checklist

- ❑ See "General Prerequisites" on page 29.
- ❑ The ALLOW AUDIT PASSWORDS console parameter must be ON for you to log in to a volume audit trail on that server.

Warning

The server's NetWare Enhanced Security configuration requires using NDS rights-based access control to protect audit data. Do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console), because this violates the assumptions under which the server was evaluated.

Procedure

Procedure

1. **Choose "Auditor volume login" in the "Available audit options" menu and press** Enter**.**

   AUDITCON prompts you to enter the volume audit password.

2. **Enter the volume audit password and press** Enter **to log in to the current volume's audit trail.**

   AUDITCON does not echo your password to the screen.

If your login is successful, AUDITCON displays menu 101, which provides the complete list of audit options for the audit trail.

If you have the wrong password or audit passwords are disabled for your current server, AUDITCON displays an error report.

Because password-based access to audit trails is not permitted in NetWare Enhanced Security configurations (ALLOW AUDIT PASSWORDS is OFF), entry of a volume password in NetWare Enhanced Security configuration will always fail. In that event, an error report is displayed.

If you can't log in to the audit trail, and you do not have NDS rights to the volume Audit File object, see your system administrator.

3. **Press** Enter **to return to menu 103.**

Restarting Volume Auditing

This menu item appears in menu 101A when the volume audit trail has overflowed. You must manually restart volume auditing using this function before nonadministrative users can use the volume again.

Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ You must have Write rights to the Audit File object Audit Policy property or have logged in with a level 2 password in order to restart volume auditing.

Procedure

1. **From menu 101A, choose "Restart volume auditing."**
2. **Press** Enter**.**

   If AUDITCON is able to restart volume auditing, it will return to menu 101.

   If it is unsuccessful, an error is displayed explaining why the restart failed, and AUDITCON returns to menu 101A.

Displaying Volume Audit Status

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29.
- ❑ In order to display the volume audit status, you must have Read or Write rights to the Audit Policy property of the Audit File object, or have Read or Write rights to the Audit Contents property of the Audit File object, or have logged in with a level 1 password.

Procedure

Procedure

1. **You can invoke this display from various places in the volume audit menu tree. For example, choose “Display audit status” in menu 101. AUDITCON then displays menu 200.**

   This is a read-only display that presents the audit status for your current volume audit trail.

2. **Press** Esc **to return to the calling menu.**

Figure 4-9
Menu 200: Audit Status

AUDIT STATUS	
Auditing status:	On
Audit file size:	2203
Audit file size threshold:	921600
Audit file maximum size:	1024000
Audit record count:	10

The “Audit status” menu displays the following status information for the current volume audit trail:

Audit Status information	Description
Auditing status	Shows as ON if auditing is enabled for the selected volume audit trail, or OFF if auditing is not enabled.
Audit file size	Shows the size, in bytes, of the current audit file.
Audit file size threshold	Shows the configured size at which the server sends warning messages to the server console and system log file.
Audit file maximum size	Defines the nominal maximum size for the audit file.
Audit record count	Defines the number of audit records in the current audit file.

This display does not define the complete status of a volume audit trail. See “Changing a Volume Audit Configuration” on page 47 for more information on viewing and setting the audit configuration.

Enabling Volume Auditing

The server is installed with auditing disabled for each volume. You must enable volume auditing to begin accumulating volume audit data.

The first time you enable auditing, AUDITCON creates an Audit File object for the volume audit trail. This Audit File object remains in place when you disable auditing.

A common usage profile is to enable auditing once, then leave auditing enabled while you configure (and reconfigure, as necessary) the specific volume events, users, directories, and files you want to audit.

Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ You must have the Read right for the Volume object's Audit File Link property. This is necessary for AUDITCON to determine the existence of an Audit File object for the volume.
- ❑ If an Audit File object does not already exist for the volume, you must have the Write right to the Volume object's Audit File Link property to modify the volume's Audit File Link to point to the Audit File object.
- ❑ If an Audit File object does not already exist for the volume, you must have the Create object right to the container object where the Volume object is located.

Procedure

1. **Run AUDITCON at a trusted workstation.**

   AUDITCON displays the current server and volume in the header area at the top of the screen.

2. **Choose the server and volume to be audited, as described in “Selecting an Alternate Server” on page 38 and in “Choosing an Alternate Volume” on page 40.**

3. **To enable auditing of a volume, choose “Enable volume auditing” in the “Available audit options” menu.**

   This option is available only in menu 102 (when auditing is not already enabled for the volume). AUDITCON checks the volume’s Audit File Link to determine whether the current volume already has an Audit File object; if so, then AUDITCON continues with Step 5.

4. **If the volume does not have an Audit File object (for example, auditing was not previously enabled for this volume), AUDITCON creates an Audit File object in the NDS container where the volume is stored.**

   The name of the Audit File object is “AFO*id_volname*”, where *id* is a counter used if there is already an object with the desired name, and *volname* is the name of the volume.

For example, if the volume name is ALPHA_SYS.ACME, then the Audit File object is named AFO0_ALPHA_SYS.ACME, or if that object already exists, then AFO1_ALPHA_SYS.ACME.

If the concept of an independent auditor (“Independent Control of Different Audit Trails” on page 13) is important to you, you might want to set the Access Control List and Inherited Rights Filter for the Audit File object to prevent access by administrators who are not auditors, as described in “Creating the Auditor Account” on page 10.

AUDITCON then builds links from the Audit File object and Volume object to each other.

As described in “Controlling Access to Online Audit Data” on page 17, the server gives you the Supervisor object right to the Audit File object, and the Write right to the ACL property. In addition, AUDITCON gives you Read and Write rights to the Audit File object Audit Policy property, and the Read right to the Audit Contents property. See “Controlling Access to Online Audit Data” on page 17 for information on giving other auditors rights to the Audit File object.

5. AUDITCON enables auditing for the volume and returns to menu 101.

When auditing is enabled for the first time on a volume, there are no events, files, or users selected. You should continue by using menu 497, 498, or 499 to select the desired audit events, files, and users.

When the server creates the audit file, it defines a password hash that cannot be matched by a hashed password submitted by AUDITCON. If you want to permit password-based access to the volume audit files, you must (1) set the console parameter ALLOW AUDIT PASSWORDS=ON and (2) use AUDITCON (“Auditing configuration” menu, “Change audit password” or “Set audit password” submenu) to set an audit password for the audit files. (You cannot configure the server to use audit passwords if you are using the server in a NetWare Enhanced Security configuration.)

Changing a Volume Audit Configuration

As auditor, it is your responsibility to review your organization's auditing requirements and identify an auditing strategy for your network. This can range from auditing nothing to auditing all events for all users. It all depends on what you want to accomplish with auditing.

One advantage of auditing, even if you audit only a few events (for example, logins), is that it can help deter browsing and probing by logged in users.

This section describes how you can use AUDITCON's audit configuration menu to

- Define what information is audited by the server (events, files / directories, and users)
- Define how audit files are handled (size, threshold, and rollover handling)
- Set audit passwords
- Disable auditing
- Recover from full volume audit trails

Prerequisites

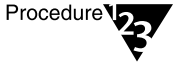
- ❑ See "General Prerequisites" on page 29.
- ❑ To examine the auditing configuration in a NetWare Enhanced Security configuration, you must have the Read right to the Audit Policy property of the Audit File object associated with the volume you want to audit.
- ❑ To change the auditing configuration in a NetWare Enhanced Security configuration, you must have the Write right to the Audit Policy property of the Audit File object associated with the volume you want to audit.

- ❑ To examine or change the audit configuration in a network that is not in the NetWare Enhanced Security configuration (that is, audit passwords are enabled at the server), you must have supplied the correct password.

  If the audit file is configured for level 2 passwords, and you don't have access through NDS rights, then you must have the level 2 password to modify the auditing configuration. If you've logged in with a level 1 password, AUDITCON prompts for the level 2 password after each operation. These screens are not shown in the following section because they don't pertain to the NetWare Enhanced Security Configuration. See "Controlling Access to Online Audit Data" on page 17 for more information.

- ❑ Determine what actions you want to perform (for example, which users to audit, how large you want the audit file to be) before you run AUDITCON.

Procedure



1. Choose "Auditing Configuration" from the "Available audit options" menu (101).

AUDITCON displays menu 497, 498, or 499, which list more configuration options, depending on the setting of the ALLOW AUDIT PASSWORDS option and whether you have sufficient rights to the Audit File object. See "Top-Level Menus" on page 34 for the definition of sufficient rights.

Table 4-2 summarizes the algorithm AUDITCON uses to determine which menu it will display, based on the above two variables. Entries in italics will not occur in the NetWare Enhanced Security configuration.

Table 4-2
Volume Audit Configuration Menu Selection

Allow Audit Passwords = ON	Sufficient Rights	Menu
Yes	*Yes*	*497*
Yes	*No*	*498*
No	Yes	499
No	No	499

Figure 4-10

Menu 497: Auditing Configuration

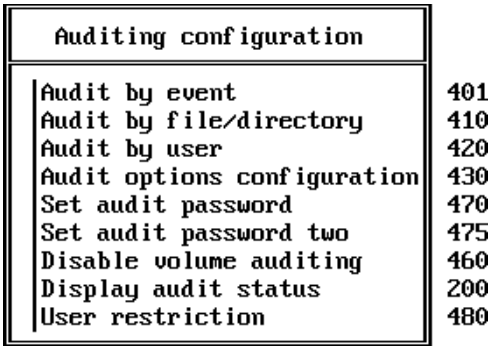


Figure 4-11

Menu 498: Auditing Configuration

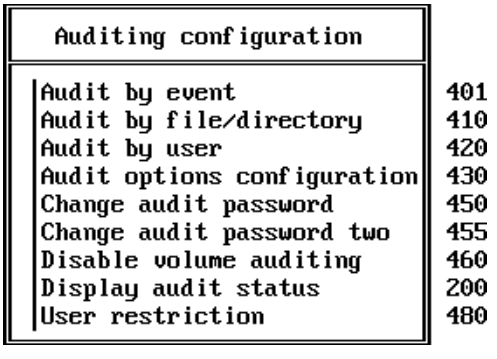
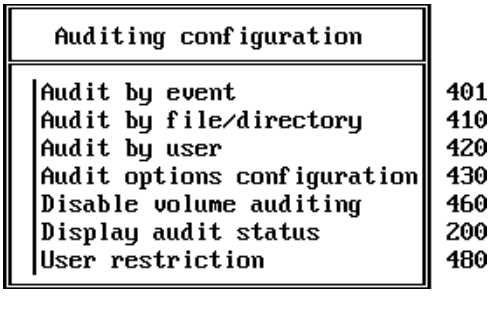


Figure 4-12

Menu 499: Auditing Configuration



2. **Choose the desired configuration option, and press** Enter**.**

   The first three entries (audit by event, file / directory, and user) allow you to preselect the events that the server will record in the audit file.

   Other entries allow you to define how the server manages audit files, to set passwords, to disable auditing, and to display the current audit status. These submenus are addressed in the following sections.

When you make changes to the volume audit configuration, you may receive a message that AUDITCON was unable to update the Audit File object. If this occurs, your configuration changes could be lost.

Audit by Event

This section describes how you preselect file, queue management, server, and user audit events.

Preselection is the operation of telling the server, in advance, which types of audit events you want the server to record in an audit file. The server records the events you have preselected and ignores other events.

By preselecting the events that are important in your organization, you conserve the disk space and processor cycles required to record the other potential audit events.

Ten of the file system events described in this section permit options for user and / or file preselection as part of event selection. For example, “file open–user and file” will cause the server to record file opens only for selected users and only for selected files. For the remaining volume events, the default is that events you select will be recorded for all users of the volume. If you want to audit only certain specific users, you should

- Preselect the users whose actions you want to record as described in “Audit by User” on page 67.
- Choose the “user *or* file” option for the desired event if the event permits a choice among “user *and* file,” “user *or* file,” or “global” preselection options.

- Set the “User restriction” flag using the “User Restriction” menu shown in Figure 4-24.

You cannot subsequently generate audit reports for events or users that were not preselected for auditing when the event occurred. For example, if you want to review logins made by a user two weeks ago, but you did not have logins preselected at that time, you will not be able to generate an audit report for these events.

You must balance your anticipated need of certain audit information with the resources required to audit those events.

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.

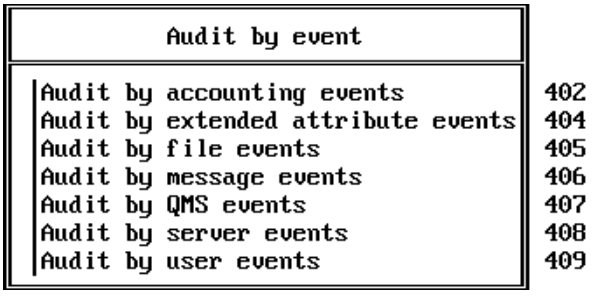
Procedure

Procedure

1. Choose “Audit by event” from the “Auditing configuration” menu (497, 498, or 499).

AUDITCON displays menu 401, which lists the classes of audit events that you can preselect for auditing.

Figure 4-13
Menu 401: Audit by Event



The following list introduces these seven classes of events and gives examples of the types of events that are included in each class.

These events are usually associated with user actions performed at client workstations, and the audit record includes the identity of the user that requested the service.

Event Class	Description
Accounting events	Accounting events include operations to get and set account charges. Accounting events are always stored in the audit trail of volume SYS:. For instructions, see “Audit by Accounting Events” on page 53.
Extended attribute events	Extended attribute events include operations to get and set file extended attributes. For instructions, see “Audit by Extended Attribute Events” on page 54.
File events	File events include operations by network users on files or directories in the current volume. These include activities such as creating or deleting a directory, and creating, opening, closing, reading, writing to, and salvaging files. For instructions, see “Audit by File Events” on page 55.
Message events	Message events include operations to read and write interconnection messages. Message events are always stored in the audit trail of volume SYS:. For instructions, see “Audit by Message Events” on page 59.
QMS events	Queue Management Services (QMS) events include operations on the server's queues, such as requests to create or destroy a print queue. QMS events are always stored in the audit trail of volume SYS:. For instructions, see “Audit by QMS Events” on page 60.

Event Class	Description
Server events	This class of events includes actions performed at a specific server, such as server console commands, mounting a volume, or shutting down a server. For instructions, see “Audit by Server Events” on page 61.
User events	User events include activities such as bindery logins and logouts and trustee assignment changes. For instructions, see “Audit by User Events” on page 63.

Note

If you are configuring a volume other than SYS:, the menu items “Accounting Events,” Message Events,” and “QMS events” will not be present.

2. **After preselecting events to be audited, press** Esc **to return to the “Auditing configuration” menu (497, 498, or 499).**

Audit by Accounting Events

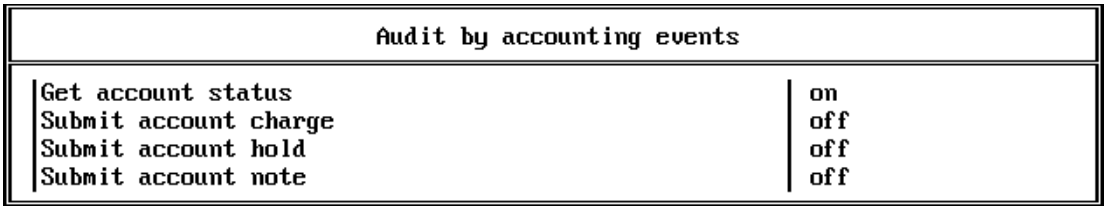
Procedure

Procedure

1. **From the “Audit by event” menu (401), choose “Audit by accounting events” and press** Enter **to edit the list of preselected accounting events.**

   AUDITCON displays menu 402, which lists the four accounting events.

Figure 4-14
Menu 402: Audit by Accounting Events



2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

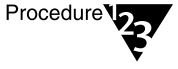
   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

   If level 2 passwords are enabled, the user does not have NDS access, and the Allow Audit Passwords option is set to ON, AUDITCON will prompt for the level 2 password before making the change.

Audit by Extended Attribute Events

Procedure



1. **Choose "Audit by extended attribute events" from the "Audit by event" menu (401) and press** Enter **to edit the list of preselected extended attribute events.**

   AUDITCON displays menu 404, which lists the four extended attribute events.

Figure 4-15
Menu 404: Audit by Extended Attribute Events

```
                Audit by extended attribute events

Duplicate extended attribute                    on
Enumerate extended attribute                    off
Read extended attribute                         off
Write extended attribute                        off
```

2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Audit by File Events

Warning

After you select file events, you must also go to the "Audit by File/Directory" menu shown in Figure 4-21 and/or the "Audit by User" menu shown in Figure 4-22 and in Figure 5-13 if you chose any "file and user" or "file or user" events. Selecting "file and user" or "file or user" events without selecting any files or users will not cause the recording of any audit events.

Procedure

Procedure

1. **Choose "Audit by file events" from the "Audit by event" menu (401) and press** Enter **to edit the list of preselected file events.**

   AUDITCON displays menu 405, which lists basic file events, basic directory events, and assorted other events. Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up, Page Down, and arrow keys.

Figure 4-16
Menu 405: Audit by File Events

```
                    Audit by file events

 Allocate directory handle                          off
 Convert handle to directory entry                  off
 Create directory - global                          off
 Create directory - user and directory              off
 Create directory - user or directory               off
 Delete directory - global                          off
 Delete directory - user and directory              off
 Delete directory - user or directory               off
 File close - global                                off
 File close - user and file                         off
 File close - user or file                          off
 File create - global                               off
 File create - user and file                        off
 File create - user or file                         off
 File delete - global                               off
▼File delete - user and file                        off
```

The following events can be displayed by scrolling the "Audit by file events" screen:

File delete - user or file
File open - global
File open - user and file
File open - user or file
File purge
File read - user and file
File read - user or file
File rename / move - global
File rename / move - user and file
File rename / move - user or file
File salvage
File search
File write - user and file
File write - user or file
Generate directory base and volume number
Get entry access rights
Get reference count for directory entry
Get specific information for entry
Get user's effective rights
Lock file
Modify directory entry - global
Modify directory entry - user and file
Modify directory entry - user or file
Obtain directory information
Scan deleted files
Scan trustee list
Scan volume's user disk restriction
Search specified directory
Set compressed file size
Set directory handle

For file and directory auditing, the server provides a highly flexible selection mechanism that you can use to preselect specific file system events, generated by specific users, for accesses to specific files or directories. These preselection options (global, user and file, user or file) are described in the following list:

Global. When you choose a global event (for example, "File open-global"), the server will audit all instances of that event (for example, file opens) in the current volume, for all users, for all files. Thus, when any user opens any file, the server will append an audit record to the volume audit trail that identifies the file open, the user, and the file.

To cause global auditing of a file system event, you only need to choose the global event, for example, "File open - global"). You do not need to select specific files or users.

User and File. When you choose a user *and* file event (for example, "File open - user and event"), the server audits the event only when it was performed by an audited user to an audited file or directory.

Table 4-3 shows the audit events that will be recorded if you select the "File open - user and file" event, users ANN and BOB, and file FOO.EXE and BAR.DAT for auditing.

Table 4-3
Examples of User and File Preselection

User Open	Of File	Audited?
ANN	FOO.EXE	Yes
ANN	BAR.EXE	No
BOB	BAR.XXX	No
BOB	BAR.DAT	Yes
CHARLES	FOO.EXE	No
CHARLES	BAR.XXX	No

To configure "user and file" auditing, (1) preselect the user and file event, (2) preselect the list of files and directories to be audited ("Audit by File / Directory" on page 64), and (3) preselect the list of users to be audited ("Audit by User" in this chapter or "Audit by User" in Chapter 5.).

User or File. When you select a user or file event (for example, "File open - user or file"), the server will audit the event when it is performed by an audited user or is performed to an audited file.

For example, Table 4-4 shows examples of the audit events that will be recorded if the "File open - user or file" event, users ANN and BOB, and file FOO.EXE and BAR.DAT are selected for auditing.

Table 4-4
Examples of User or File Preselection

User Open	Of File	Audited?
ANN	FOO.EXE	Yes
ANN	BAR.EXE	Yes
BOB	BAR.XXX	Yes
BOB	BAR.DAT	Yes
CHARLES	FOO.EXE	Yes
CHARLES	BAR.XXX	No

To configure "user or file" auditing, (1) preselect the user or file event, (2) preselect the list of files and directories to be audited ("Audit by File / Directory" on page 64), and (3) preselect the list of users to be audited ("Audit by User" in this chapter or "Audit by User" in Chapter 5).

When using "user and file" or "user or file" events, see the cautions in "Audit by User" on page 67 or "Audit by User" on page 161. The set of users you identify is global; that is, they will be audited on all volumes, containers, and servers in your Directory tree, not just on a particular volume.

Global auditing, particularly of common events such as file opens, can result in a high volume of audit events. Unless you closely monitor the status of the audit files that are collected by the server, this can cause the server to automatically take the volume offline when the audit files or volume are filled.

2. Move the cursor to each event and press F10 **to toggle it to the desired state (for example, OFF to ON).**

Enabling one event (for example, "File open - user or file") will cause related events (for example, "File open - global") to automatically change state.

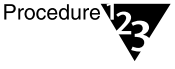
3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Audit by Message Events

Procedure



1. **Choose "Audit by message events" from the "Audit by event" menu (401) and press** Enter **to edit the list of preselected queue events.**

   AUDITCON displays menu 406, which lists the five message events.

Figure 4-17
Menu 406: Audit by Message Events

```
                    Audit by message events

Broadcast to console                                    off
Disable broadcasts                                      off
Enable broadcasts                                       off
Get broadcast message                                   off
Send broadcast message                                  off
```

2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Procedure

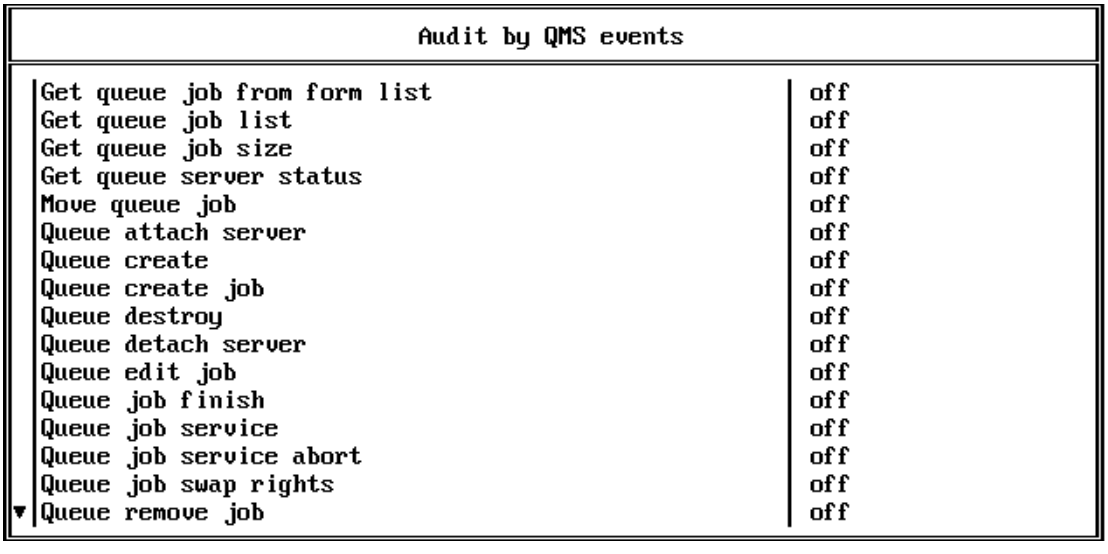
Procedure

1. **Choose "Audit by QMS events" from the "Audit by event" menu (401) and press** Enter **to edit the list of preselected queue events.**

   AUDITCON displays menu 407, which lists the events that are commonly used by network clients to submit and manage print queues.

   Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up, Page Down, and arrow keys.

Figure 4-18
Menu 407: Audit by QMS Events



The following events can be displayed by scrolling the "Audit by QMS events" screen:

Queue set job priority
Queue set status
Queue start job
Read queue job entry
Read queue status

Restore queue server rights
Set print job environment
Set queue server status

2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Audit by Server Events

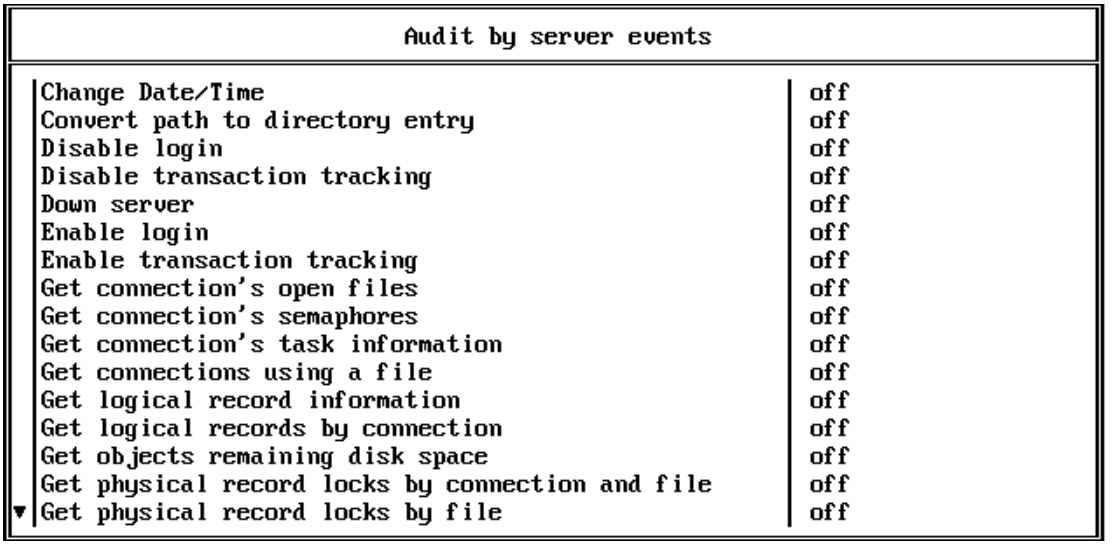
Procedure

1. **Choose "Audit by server events" and press** Enter **to edit the list of preselected queue events.**

   AUDITCON displays menu 408, which lists the server audit events. Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up, Page Down, and arrow keys.

Figure 4-19

Menu 408: Audit by Server Events



The following events can be displayed by scrolling the "Auditing by server events "screen:

Get semaphore information
Get user disk utilization
Map directory number to path
NLM add audit record
NLM add user ID record
Remote add name space
Remote dismount volume
Remote execute file
Remote load NLM
Remote mount volume
Remote set parameter
Remote unload NLM
Send console broadcast
Server console broadcast
Server console command
Terminate service connection
Verify server serial number

Volume dismount
Volume mount

2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

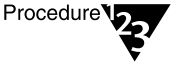
3. **When you have set and reviewed the audit event configuration, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Audit by User Events

Procedure



1. **Choose "Audit by user events" and press** Enter **to edit the list of preselected user events.**

   AUDITCON displays menu 409, which lists seven events associated with server-centric bindery login sessions.

Figure 4-20
Menu 409: Audit by User Events

```
                    Audit by user events

Clear connection                                    off
Disable account                                     off
Grant trustee                                       off
Log in user                                         on
Log out user                                        off
Remove trustee                                      off
User space restrictions                             off
```

2. **Move the cursor to each event and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set, and reviewed, the audit event configuration, press** Esc **to save the configuration.**

AUDITCON then displays menu 403 (shown previously) to confirm that you want to make the changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit events unchanged.**

Audit by File/Directory

This section describes how to preselect files and directories in the volume for auditing.

After you preselect a file or directory for auditing, you must also go to the "Audit by event" and "Audit by file events" menus shown in the "Changing a Volume Audit Configuration" on page 47), then choose the "user and file" or "user or file" events you want to audit. Selecting a file or directory without the associated events will not cause the file to be audited.

The server keeps file and directory audit flags in the file system, but does not save that information when you back up the volume. If you ever restore files or directories from backup, the audit flags will be lost. Consequently, you must keep a manual record of all files and directories you've preselected for auditing in order to be able to restore that information.

Table 4-5 shows a sample form that you can use when recording which files and directories have been marked for auditing. You must keep a record of all such files and directories for recovery purposes. If the system is ever restored from a full backup, you will use this list to reconstruct your audit settings. In addition, if the administrator restores files or directories from a backup, you will want to use this record to reestablish your audit settings. Failure to keep and use such a record can result in loss of audit data.

Table 4-5
Sample Format for Recording File/Directory Settings

Date	Time	Set/-Cleared?	Server	Volume	Path Name
23 Mar 95	2:50pm	Set	SERVER1	SYS:	\PUBLIC\NETADMIN.EXE
23 Mar 95	2:55pm	Set	SERVER1	ALPHA:	\USERS\SMITH
23 Mar 95	3:17pm	Set	SERVER2	ZETA:	\USERS\JONES
24 Mar 95	9:42am	Cleared	SERVER1	SYS:	\PUBLIC\NETADMIN.EXE

Table 4-5 *continued*

Sample Format for Recording File/Directory Settings

Date	Time	Set/-Cleared?	Server	Volume	Path Name
24 Mar 95	9:50am	Cleared	SERVER2	ZETA:	\USERS\JONES
24 Mar 95	1:35pm	Set	SERVER1	SYS:	\PUBLIC
24 Mar 95	1:50pm	Set	SERVER1	SYS:	\SYSTEM

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.
- ❑ You don’t need file system rights to a file or directory to select it for auditing. If you have rights to the volume audit trail, the server will list files and directories that you can select for auditing. (This does not permit you to access those files or directories, but only to enable them for auditing.)
- ❑ Determine the list of files and directories you want to audit before you run AUDITCON.

Procedure

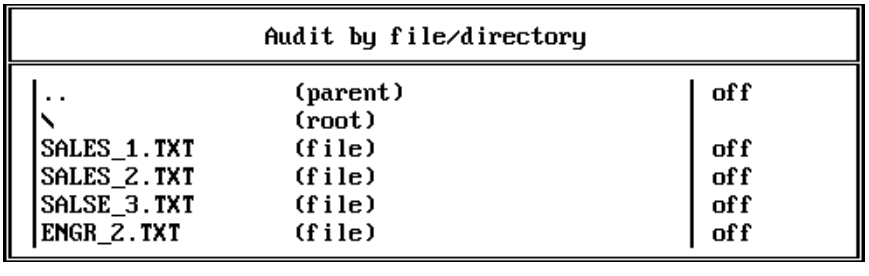
Procedure

1. **Choose “Audit by file/directory” from the “Auditing configuration” menu (497, 498, or 499).**

   AUDITCON displays menu 410, which lists the contents of the current directory of the current volume. The following menu shows an example of a display for the PUBLIC directory.

Figure 4-21

Menu 410: Audit by File/Directory



Accesses to a file are subject to auditing if either (a) the file itself is preselected for auditing or (b) the containing directory is preselected.

For example, accesses to the file AUDITCON.EXE are subject to auditing because the file itself is preselected. Accesses to files in BACKUP, for example, BACKUP\FILE1 and BACKUP\FILE2, are subject to auditing because the BACKUP subdirectory is preselected for auditing.

However, accesses to BACKUP\DIR1\FILE1 are not subject to auditing unless the BACKUP\DIR1 subdirectory is preselected. Thus, setting the audit preselection flag for a directory only affects the audit status of files that are immediately contained in that directory.

Auditing is also subject to the "File and user" and "File or user" criteria that were selected.

When you create a subdirectory, the new subdirectory inherits the value of the audit preselection flag from its parent directory. Thus, if you create the BACKUP\DIR2 and BACKUP\DIR2\DIR3 subdirectories, they inherit the audit flag from the BACKUP directory. Any files in these subdirectories are subject to auditing.

The inheritance of audit preselection flags applies only when a subdirectory is created. If you preselect the BACKUP directory for auditing, the audit flag *does not* flow down to existing subdirectories, such as BACKUP\DIR1.

Because audit preselection flags are not saved when you back up a volume, and because audit flags are inherited when you create a subdirectory within an audited directory, you can end up auditing more directories than shown in your manual audit log.

For example, if you flag the directory \A\B for auditing and then create the \A\B\C subdirectory, \A\B\C will inherit the audit flag from \A\B. If the volume is then backed up and restored, your audit flag log only shows \A\B as being audited.

To prevent problems with this feature, log any important subdirectories that inherit audit flags. If you log enough information to manually restore the audit flags for all directories you want to audit, you don't need to be concerned about the loss of audit flags for other directories.

2. **Move through the Directory tree by pressing** Enter **to browse a subdirectory in the current menu, choosing ".." to browse**

the parent directory, or choosing "\" to return to the root directory.

The AUDITCON window displays only 16 entries at a time, so you might need to use the arrow keys to scroll through a directory.

3. **Move the cursor to a desired entry and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

4. **When you have set and reviewed the audited files and directories, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

5. **Choose "Yes" to save the changes and return to menu 410, or choose "No" to leave the audit events unchanged.**

Audit by User

This section describes how you preselect specific users for volume auditing. When you preselect a user for auditing, the server associates this audit flag with the NDS User object. The server then consults this per-user audit flag as follows:

- For the ten file system events that allow user and/or file preselection, the server will record the "user and file" events only if both the user and file are selected for auditing. The server will record "user or file" events if either the user or the file is selected for auditing. See "Audit by Event" on page 50 for more information.

- For all other volume events, if the "User restriction" flag is selected for the volume audit file, the server records the events only for preselected users. See "User Restriction" on page 84 for more information.

By default, the "User restriction" flag is not set, so selection by user only applies to the "user or file" and "user and file" events. If you want to preselect by user for all volume events, you must set the "User restriction" flag for the volume.

After you preselect a user for auditing, you must also perform the following tasks to ensure that the user's actions are recorded in the volume audit file:

- For any of the ten file system events that permit user and/or file preselection, you must also go to the "Audit by event" and Audit by file events" menus to select the "user and file" or "user or file" events you wish to audit. For these events, selecting a user without the associated events and files will not cause the user's file access to be audited.

- For all other volume events, you must set the "User restriction flag" to "Yes," as described in "User Restriction" on page 84.

When you select a user for volume auditing, the selection applies to all volumes and containers in the network where preselection is in effect. For example, selecting BOB for certain "user or file" events on volume SYS: also selects BOB for all "user or file" and "user and file" events selected for all other volumes on all other servers in the network. Similarly, selecting JANE for volume auditing will cause JANE to be audited on all containers where the "User restriction" flag is set to "Yes."

A side effect of this is that you can select a user for auditing using either the "Audit by user" menu or the corresponding "Audit by DS users" menu under NDS auditing. Both have the same effect.

The server keeps user audit flags in the associated User objects in NDS but does not save that information when you back up NDS. If you ever restore NDS from a backup, the audit flags will be lost. You must keep a manual record of all users you've preselected for auditing in order to restore that information.

If an auditor has rights to audit any volume or container in the network, that auditor can enable or disable auditing for any user in the NDS tree.

Table 4-6 shows a sample format for recording which users have been marked for auditing. You must keep a record of all such users for recovery purposes. If NDS is ever restored from a full backup, you will use this list to reconstruct your audit settings. Failure to keep such a record and use it can result in loss of audit data.

Table 4-6
Sample Format for User Settings

Date	Time	Set/Cleared	NDS User Object Name
23 Mar 96	3:45pm	Set	CN=SALLY.O=ACME
23 Mar 96	3:48pm	Set	CN=HENRY.O=ACME

Table 4-6
Sample Format for User Settings

Date	Time	Set/Cleared	NDS User Object Name
24 Mar 96	8:12am	Set	CN=FRED.OU=SALES.O=ACME
25 Mar 96	11:32am	Clear	CN=SALLY.O=ACME
25 Mar 96	11:50am	Set	CN=JULIE.OU=ENGR.O=ACME

Because NDS is a distributed system and some servers might be offline at any given time, selecting a user for auditing might involve a long delay before NDS can synchronize this information throughout the network. See “Security Supplement to Managing the Novell Directory Tree” in *NetWare Enhanced Security Administration* for information on how to determine that a change has been synchronized to all replicas of the partition.

Prerequisites

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.
- ❑ Determine which users you want to audit.

Procedures

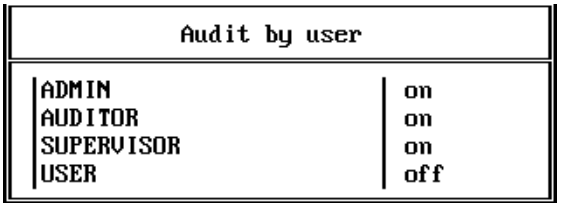
1. Choose “Audit by user” from the “Auditing configuration” menu (497, 498, or 499).

AUDITCON displays menu 420, which lists the users on the server. The list of users displayed is those users in the default bindery context for the server where the volume is located.

The AUDITCON window shows only 16 entries at a time, so you might need to use the arrow keys to scroll through the list of users.

The list of users shown is not the complete list of potential users of the volume. To see (and mark) users other than those listed here, see “Audit by User” on page 161. You will be working in the NDS auditing menu tree.

Figure 4-22
Menu 420: Audit by User



2. **Move the cursor to a desired entry and press** F10 **to toggle it to the desired state (for example, OFF to ON).**

3. **When you have set and reviewed the list of audited users, press** Esc **to save the configuration.**

   AUDITCON asks you to confirm the changes.

4. **Choose "Yes" to save the changes and return to menu 420, or choose "No" to leave the audit events unchanged.**

Note

In addition to this method of preselecting users for auditing, you can also use an alternate method within the container auditing menu. See "Audit by User" on page 67.

Setting the audit flag on the USER_TEMPLATE user will not cause automatic auditing of newly created users. When a new user is created, you must preselect the User object if you want that user's actions audited.

Audit Options Configuration

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 47.

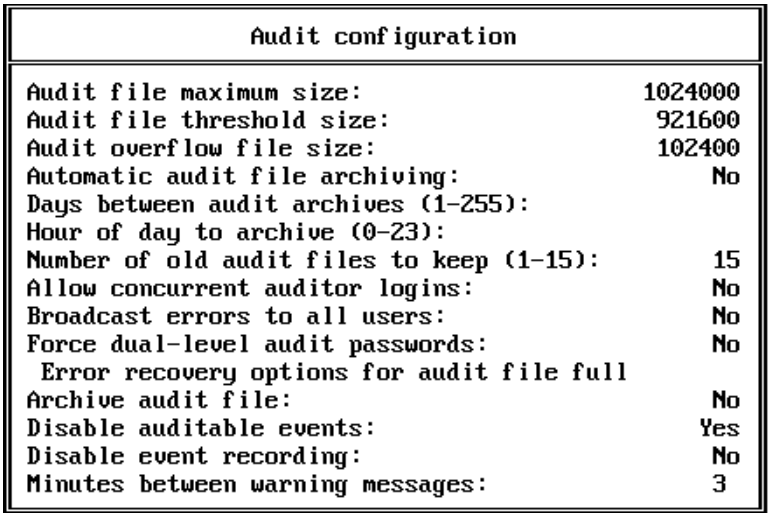
Procedure

Procedure

1. **Choose "Audit options configuration" from the "Auditing configuration" menu (497, 498, or 499).**

   AUDITCON displays menu 430, which defines the current audit configuration for the volume audit trail.

Figure 4-23
Menu 430: Audit Configuration



The line “Force dual-level audit passwords” is omitted if the ALLOW AUDIT PASSWORDS console parameter is OFF, as required in the NetWare Enhanced Security configuration.

The following list describes the available configuration parameters. The server has two mechanisms for archiving the current audit file to an old audit file, and creating a new audit file. These are (1) automatic archiving, which causes the server to archive the audit file after a specified number of days, and (2) file overflow, which causes the server to archive the audit file when the current audit file exceeds the specified maximum size.

In either case, the server closes the current audit file, archives the contents to an old audit file, and opens a new current audit file.

The terms *archive* and *archiving* are used here to refer to a mechanism for rolling over the current audit file and starting a new current audit file. The process of saving copies of online audit files to removable media is referred to as *backup*.

Audit File Size Parameter	Description
Audit file maximum size	This parameter defines the maximum size (in bytes) of the audit file. However, because of the way the server processes audit events, the actual audit file size might slightly overrun this value. For example, if you intend to copy online audit files onto 1.44 MB diskettes, you might want to set the maximum file size to approximately 1.3 MB.
Audit file threshold size	This parameter defines the file size threshold (in bytes) at which the server sends a warning message to the server console and an entry to system log file. The threshold should be approximately 90% of the maximum file size. For example, a maximum setting of 1,000,000 bytes should have a threshold setting of 900,000 bytes.

Audit File Size Parameter	Description
Overflow audit file size	The audit overflow file holds audit data when the current audit file is full and the “Disable auditable events” option has been selected (see below). This file should be large enough to hold the maximum size audit record for each service process on the server, plus a reasonable amount to store records recording the auditor’s actions to correct the overflow situation. The default setting is 100K (102400 bytes). Disk space for the overflow audit file is preallocated. The space you allocate is unavailable for other purposes. Therefore, you should be cautious when setting this value high to avoid running out of space for audit records. If you set it too high, you will waste space. These are the maximum sizes: ◆ Volume audit record: 1024 bytes ◆ Container audit record: 4096 bytes ◆ External audit record: 4096 bytes You can find the number of service processes on the server using the MONITOR utility or by typing “SET MAXIMUM SERVICE PROCESSES” on the server console. The parameter default is 40. If your MAXIMUM SERVICE PROCESSES parameter is set to 60, the overflow audit file size should be set to at least 61,440 (60x1024) for a volume or 245,760 (60x4096) for a container or external audit trail.

Audit File Size Parameter	Description
Automatic audit file archiving	Set this parameter to “Yes” to cause the server to periodically archive the current audit file to an old audit file, as specified by the “Days between audit archives” setting. (The term *archive* refers to rolling the current audit file over to a new audit file, and does not imply any offline backup of the audit data, for example, to removable media). This setting ensures that the server maintains old audit information, but it might require large amounts of disk space, depending on the number of old audit files you decide to keep on the server. Use this parameter with the next three options. If you use this parameter, it can cause loss of audit data if the automatic archive overwrites old audit files that have not been previously backed up. For this reason, its use is not recommended in the NetWare Enhanced Security configuration.
Days between audit archives (1-255)	Set the number of days the server will collect data in the current audit file before automatically archiving the file. You can select 1-255 days; the default is 7 days. This option is valid only when the “Automatic Audit File Archiving” is set to Yes.

Audit File Size Parameter	Description
Hour of day to archive	Set the hour of the day for auto archiving to take place. You can select any hour of the day, using a 24- hour clock (0-23). The default is 0 (midnight). The archive will usually begin a few seconds after the specified hour. This option relates only to periodic archiving of the audit file. It is valid only after you have turned on the auto-archive option.
Number of old audit files to keep (1-15)	This parameter defines how many old audit files the server will maintain online. When the server needs to archive the current audit file (either because of size overflow or periodic archiving), it compares the actual number of old audit files with this setting. If the actual number of old audit files is less than this value, the server creates another old audit file. If the number of old audit files has reached this value, the server performs overflow recovery according to one of these settings: ◆ Archive audit file ◆ Disable auditable events ◆ Disable event recording. **Warning:** If you reduce the number of old audit files, then audit files in excess of the new number allowed will be deleted. Be sure you have backed up your old audit files before reducing the maximum number retained.

Audit File Size Parameter	Description
Allow concurrent auditor logins	Choose “Yes” to allow more than one auditor to have access to a volume audit trail at the same time.
Broadcast errors to all users	Choose “No” if you want error messages sent only to the server console. This is the required value for NetWare Enhanced Security configurations. Broadcasting error messages increases network traffic and can lock users' workstation screens until they press Ctrl+Enter (or choose “OK” if running Microsoft* Windows*).
Force dual-level audit passwords	Choose “Yes” to require separate passwords for reading the audit data (level 1) and writing the configuration data (level 2). You are prompted to enter a level 2 password when you set this field to “Yes” for the first time. When you change the audit configuration, AUDITCON prompts for a level 2 password. This line will be blank if the ALLOW AUDIT PASSWORDS console parameter is set to off, as required in the NetWare Enhanced Security configuration.

The server provides three mutually exclusive options for handling full audit files and write errors caused by a full disk volume. The options are: “Archive audit file”, “Disable auditable events”, and “Disable event recording.” The default is “Disable auditable events”.

You can select only one of these options at a time. As soon as you select any one, the other two will be turned off. If you don’t select any, then “Disable auditable events” will be selected for you.

These options are explained in the following table.

Full Audit File Option	Description
Archive audit file	With this setting, the server archives the current audit file (that is, changes the current audit file to an old audit file) and creates a new audit file. If necessary (because the maximum number of old audit files already exists), the server deletes the oldest of the old online audit files. This option is not recommended for use in NetWare Enhanced Security networks because it might result in the loss of audit data.

Full Audit File Option	Description
Disable auditable events	This setting lets the server place the volume in an overflow state when (a) the current audit file has reached the “Audit file maximum size” or (b) it cannot write to the current audit file (for example, the volume is full). The server doesn’t try to roll over to a new audit file, even if there is disk space for archiving the current audit file. When a volume is in an overflow state, any NCP request which is potentially auditable is not allowed, even if that event would not cause an audit record to be generated. For example, in an overflow state, the server won’t permit users to perform any file open operations on the volume, even if the event is not preselected for auditing. The effect is essentially the same as if the overflowed volume had been dismounted. To recover, you must reset the current audit file (see “Reset Audit Data File” on page 132. If volume SYS: overflows, the server permits an audit administrator to perform a read-only login to the server to reset the audit file. Other users aren’t permitted to log in while volume SYS: is in an overflow state. This is the only overflow option that guarantees that you will not lose audit data. Consequently, if collecting audit data is very important (such as in a NetWare Enhanced Security network), you should use this setting, even though it might inconvenience users who need to access the volume.

Full Audit File Option	Description
Disable event recording	This setting lets the server turn off auditing and stop entering new audit records into the current audit file when it reaches the maximum size limit or when an unrecoverable write error occurs for the audit file. The server doesn't try to create a new audit file, even if there is disk space to archive the current audit file. You must reset the current audit file in order to re-enable event recording. Until you re-enable event recording, users can access the volume without any audit coverage. Consequently, this setting is not recommended for use in NetWare Enhanced Security networks because it can result in audit data being lost.
Minutes between warning messages	The server sends warnings to the console at this frequency if (a) the audit file is full and (b) the overflow option is configured to either "Disable auditable events" or "Disable event recording". If you have the "Archive audit file" option configured, then a warning message is sent when the audit file is almost full, but there is no additional message when the archive occurs.

2. Move the cursor to the field you want to change and enter the new configuration value.

For numeric fields (for example, "Audit file maximum size"), type the new value into the field over the previous value, then press Enter. For "Yes / No" settings, type "Y" or "N" to change the value.

Depending on the context of your change, the server might modify other values on the configuration screen. For example, if you set "Automatic audit file archiving" to "No", the server will

blank out the entries for "Days between audit archives" and "Hour of day to archive."

3. **If you enable "Force dual-level audit passwords" and the ALLOW AUDIT PASSWORDS option is set to ON, AUDITCON will immediately prompt you (twice) to enter the new level 2 password.**

These menus are not shown here, because audit passwords are not permitted in NetWare Enhanced Security networks.

4. **Review the settings on the current screen, and change any settings as required.**

5. **Press** Esc **to exit the menu.**

   AUDITCON asks you to confirm the changes.

6. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the audit configuration unchanged.**

If you intend to back up audit files to high-density (1.44 MB) diskettes, set the maximum size of the audit file to approximately 1.3 MB to ensure that the audit file will fit on the disk.

Audit files consume disk resources that might be needed by other users. Before you define the number and size of audit files, discuss your projected disk space requirements with an administrator for the server. If you set the audit file size too small, you risk shutting down the server volume or losing audit data, depending on the overflow option you've configured.

The server's NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. Do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON), because this violates the assumptions under which the server was evaluated.

The server does not provide any locking mechanism to prevent multiple auditors from simultaneously attempting to change volume, container, or external audit configuration data. If this occurs, the last auditor to write the audit configuration might overwrite changes made by other auditors. If more than one auditor has rights to modify the audit configuration, you must institute procedural methods to control access to the Audit File object, such as selecting a single replica of the Audit File object and making all changes to that replica.

If you specify the “Disable auditable events” option, the server will stop processing auditable volume NCP™ requests when the current audit file fills up, even if there is sufficient disk space to roll over the audit file and start a new audit file. For example, you could have room for 15 online audit files, but the server will disable auditable NCP events when the current audit file fills up.

To prevent this disruption, configure automatic audit file archiving so that the current audit file will not overflow during routine operation. For example, if it normally takes two days to fill an audit file, set “Automatic audit file archiving” to ON, “Days between audit archives” to one day, and “Number of old audit files” to at least 7. To prevent audit loss, you should monitor the audit status on a regular basis, and you must clean out the old audit files before the last audit file is used.

If you configure both “Automatic audit file archiving” and the “Archive audit file” overflow option, the server will roll over the current audit file at both the appointed time and the specified file size. For example, if you're archiving audit files every Friday and the file becomes full on Thursday, the server will roll over the audit file on Thursday (overflow processing) and then again on Friday (automatic archival processing). Consequently, you might use up the configured number of old audit files (for example, 15) faster than anticipated. To prevent loss of audit data, you should monitor the audit status on a regular schedule and you must clean out the old audit files before the last file is used.

Change Audit Passwords

This section describes how the auditor can change level 1 audit passwords and level 2 audit passwords (if level 2 passwords are enabled). For information on using the password-based mechanism for accessing audit files, see “Controlling Access to Online Audit Data” on page 17.

The server’s NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. For NetWare Enhanced Security networks, do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console) because this violates the assumptions under which the server was evaluated.

Prerequisites

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.

Procedure

1. **To change the level 1 password, choose “Change audit password” from the “Auditing configuration” menu (498).**

2. **Enter the current (level 1) audit password.**

   AUDITCON does not echo any password information to the screen.

   If dual-level passwords are enabled, AUDITCON prompts you to enter the level-2 password before you can change the level-1 password. AUDITCON allows you to change the level-2 password using the same procedure used to change the level-1 password.

3. **Enter the new (level 1) audit password when prompted by AUDITCON.**

   AUDITCON prompts you twice for the new password. This ensures that the auditor did not make an error when entering the password.

   AUDITCON doesn’t check the password for length, alphanumeric characters, or other characteristics of strong passwords, nor does it ensure that it is different from the previous password. Uppercase and lowercase characters are treated identically.

Set Audit Passwords

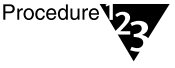
This section describes how to set level 1 audit passwords and level 2 audit passwords (if level 2 passwords are enabled). This section is applicable only if the ALLOW AUDIT PASSWORDS option is set to ON. For more information on using the password-based mechanism for accessing audit files, see “Controlling Access to Online Audit Data” on page 17.

The server’s NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. For NetWare Enhanced Security networks, do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console) because this violates the assumptions under which the server was evaluated.

Prerequisites

❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.

Procedures



1. **To set the level 1 password, choose “Set audit password” from the “Auditing configuration” menu (1497).**

   AUDITCON prompts you to enter the new (level 1) container password.

2. **Enter the new password.**

   AUDITCON does not echo any password information to the screen

   If dual-level passwords are enabled, AUDITCON prompts you to set the level 2 password before you can set the level 1 password. AUDITCON allows you to set the level 2 password using the same procedure used to change the level 1 password.

3. **Reenter the new password.**

   The dual prompt ensures that the auditor did not make an error when entering the new password.

   AUDITCON does not check the password for length, alphanumeric characters, or other characteristics of strong passwords, nor does it ensure that it is different from the previous password. Passwords are not case-sensitive.

If you use audit passwords to control access to the audit file, do not use your server password as the audit password.

If you use a password to control access to an audit file, and forget the audit password, then you must use the rights-based access, as described in “Access Controls for Online Audit Data” in Chapter 2. When you have access to the audit trail, you can reset the password as described in this procedure.

Disable Volume Auditing

When you disable volume auditing, you stop the server from recording audit events to the volume audit file, but you do not delete the Audit File object for the volume audit trail. The Audit File object remains and

is reused (to provide an initial configuration) if you re-enable auditing for the volume. After volume auditing has been disabled, it can be re-enabled using the Enable Volume Auditing menu (see “Enabling Volume Auditing” on page 44).

Prerequisites

❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 47.

Procedures

1. **Choose “Disable volume auditing” from the “Auditing configuration” menu (497, 498, or 499).**

   AUDITCON asks you to confirm that you want to disable auditing for the volume.

2. **Choose “Yes” and press** Enter **to disable auditing, or “No” to continue auditing.**

   AUDITCON returns to menu 497, 498, or 499.

User Restriction

This menu provides for setting the following audit control flags in the current volume’s Audit File object Audit Policy.

- **User Restriction.** The server provides two different methods for auditing the actions of specific users. It distinguishes between a set of ten file system events (those which permit “user or file” and “user and file” selection) and the remaining volume events.

  By default, the remaining (non-user / file) events are audited for all users. However, if you set the “User restriction” flag, the server will audit only those users who have been specifically preselected for auditing. See “Audit by User” on page 67.

- **Audit NOT_LOGGED_IN**. Before a user logs in to NDS, the server permits the user to access files in the \LOGIN directory. See “Security Supplement to Managing Directories, Files, and Applications” in *NetWare Enhanced Security Administration* for more information. By default, the server does not audit these unauthenticated user events. However, if you set the “Audit

NOT_LOGGED_IN users" flag, the server records these events in the current volume audit file.

These flags pertain only to the currently selected volume and do not affect other volume or container audit files. Unlike the per-user audit flag (which is global across the network), the "User restriction" and "Audit NOT_LOGGED_IN users" flags must be set individually for each volume and container. The two flags are independent of each other, so you can set either flag without affecting the other.

Warning

If you set the "User restrictions" flag to "Yes", you must also preselect those users you want audited, using the procedures shown in "Audit by User" on page 67 or "Audit by User" on page 161. Setting the "User restrictions" flag to "Yes" without preselecting any users will mean that only "User or File" events (where the file is preselected) will be recorded in the audit trail.

If you set the "User restrictions" flag to "Yes" but leave the "Audit NOT_LOGGED_IN users" flag set as "No", then actions of unauthenticated users will not be audited, unless they would otherwise be audited by selection of "User or File" events where the file is preselected.

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 47.

Procedures

Procedure

1. **Choose "User restriction" from the "Auditing configuration" menu (497, 498, or 499).**

   AUDITCON displays menu 480, which allows you to select the desired user restriction parameters for the volume.

Figure 4-24
Menu 480: User Restriction

```
                    User restriction

Audit NOT_LOGGED_IN users                          No
User restriction                                   No
```

2. **Review the settings on the current screen, and change any settings as required. Press "Y" to set a value to "Yes" or press "N" to set the value to "No."**

3. **When you are finished, press** Esc **to exit the menu.**

AUDITCON asks you to confirm your changes.

4. **Choose "Yes" to save the changes and return to menu 497, 498, or 499, or choose "No" to leave the user restrictions configuration unchanged.**

Generating Volume Audit Reports

AUDITCON allows you to process online and offline audit files to extract and review the information the server has collected for you. Processing consists of displaying audit information on the AUDITCON screen (viewing) and generating printable reports (printing).

This section describes how to process online audit files, either the current audit file or the old audit files that have been archived (that is, rolled over) by the server but are still maintained as audit files by the server. See "Generating Reports from Offline Audit Files" on page 122 for information on how to process offline audit files.

Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ To process online audit files, you must either have the Read right to the Audit File object Audit Contents property or have logged in to the audit trail. (To log in to an audit trail, you must enable audit passwords at the server console. This configuration is not permitted in NetWare Enhanced Security facilities.)
- ❑ You must be able to create new (temporary) files in the directory you were in when you started AUDITCON, and have sufficient disk space on that volume. These temporary files hold the audit data as it is extracted from the audit trail.
- ❑ You must have preselected events for auditing. You can view or report only those audit events that have been recorded by the server; for example, if you don't configure the server to record file open events, then you can't display any file open events. (See "Changing a Volume Audit Configuration" on page 47 for more information on preselection.)

Because AUDITCON places temporary files in the directory you were in when you started AUDITCON, and these temporary files contain audit

data, you must not generate any reports unless your current directory is protected from access by users who are not authorized to see audit data.

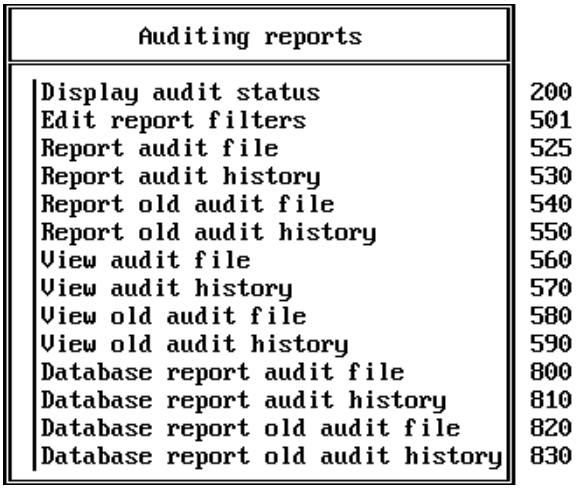
Procedure

Procedure

1. Choose "Auditing reports" from the "Available audit options" menu (101).

AUDITCON displays menu 500.

Figure 4-25
Menu 500: Auditing Reports



2. Choose the desired auditing report option, and press Enter**.**

You have several options for creating and viewing reports from the records in audit files.

- You can create filters to extract specific information (for example, users or files) from the audit file, or you can view all the records in an audit file. Unless you are just browsing the audit trail, you would normally want to define one or more report filters before you generate an audit report or view an audit file.
- You can process the current audit file (for example, "Report Audit File") or process an old audit file (for example, "Report old audit file"). References to old audit files explicitly indicate operations on one of the server's old audit files, while the other operations are implicit on the current audit file.

- You can direct output to your AUDITCON screen (for example, “View audit file”) or send the output to a file on your workstation or a directory on the server (for example, “Report audit file”).
- You can extract information about client user events (for example, “View audit file”) or extract information about auditor events (for example, “View audit history”). The audit file contains user events, while the audit history file contains a record of actions by the auditor in managing the audit trail.

  The audit history is actually included in the audit file, and is not a separate file. It is described as the audit history file for compatibility reasons.
- You can cause reports to be generated as text (for example, “Report audit file”) or in a form suitable for loading into a database (for example, “Database report audit file”).

These options are addressed in the following sections.

Edit Report Filters

The procedures described in this section allow you to generate filter files and report files on your local workstation. See your client documentation for details on how to use your workstation’s security mechanisms to protect these files.

AUDITCON lets you create filters so you can extract the specific information that you want from an audit file. If you view a report without applying a filter, AUDITCON displays the entire contents of the file.

You can create as many filters as you want to screen information in the audit file. Then, any time you want to generate a report, you can select and apply the filter.

An audit filter is an ordinary file that contains the filter information. By default, AUDITCON saves the filter file in your current working directory, which can be either a local drive or a network drive. The name of the file is typically the filter name, with a file extension of “.ARF” (for Audit Report Filter). While this allows you to create audit filters in a variety of different directories, AUDITCON does not provide a means for you to access filters in a different directory. Consequently, to use a filter that you have previously defined, you must run AUDITCON from the directory where the filter is located, or copy the filter to your current directory before you run AUDITCON. Audit report filters must be

protected from modification by storing them only in locations where they will be protected by NetWare or by client workstation access controls.

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.

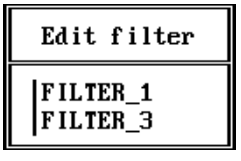
Procedure

Procedure

1. From the “Auditing reports” menu (500), choose “Edit report filters.”

AUDITCON displays menu 501, which lists the filters you have previously defined. If you have not defined any filters in the current directory, AUDITCON displays a null entry “_no_filter_”.

Figure 4-26
Menu 501: Edit Filter

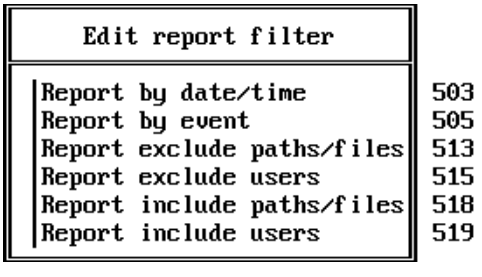


2. Highlight an entry and press either F10 **or** Enter **to select that filter for editing. Or, press** Insert **to create a new audit filter.**

In each case, AUDITCON displays menu 502, which shows the available filter criteria. The steps for creating a new filter and editing an existing filter are essentially the same.

The primary difference is that if no audit filters exist, you can press Enter to create a new audit filter, but you cannot press F10 to edit.

Figure 4-27
Menu 502: Edit Report Filter



3. **Choose an option (that is, criteria for printing an audit record) and press** Enter **to define the filter rules, described in Table 4-7.**

Table 4-7
Filter Rules

Filter Rule	Description
Report by date/time	This filter allows you to specify one or more time periods to include in a report. All audit records that match one of the time periods are a candidate for reporting. If the date/time filter is empty (that is, no times are specified), all audit records are a candidate for reporting. For instructions, see “Report by Date/Time” on page 91.
Report by event	This filter allows you to specify the types of audited events to include in a report. All audit events that match the specified events are a candidate for reporting. For example, if you specify create directory and file open events in a filter, your report will include only create directory and file open events. For instructions, see “Report by Event” on page 93.
Report exclude paths/ files	This filter allows you to specify one or more files or directories that you wish to exclude from audit reports. All other files and directories are potentially included in the report. Only those files and directories named are excluded. That is, if you exclude \FOO, that does not also exclude \FOO\BAR. For instructions, see “Report Exclude Paths/Files” on page 99.
Report exclude users	This filter allows you specify one or more users that you want to exclude from audit reports. All other users are potentially included. For instructions, see “Report Exclude Users” on page 100.
Report include paths/ files	This filter allows you to specify one or more file or directory pathnames that you want to include in the report. The default is “*”, which indicates that all files and directories are potentially reported. Only those files and directories named are included. For example, if you include \FOO, that does not also include \FOO\BAR. For instructions, see “Report Include Paths/Files” on page 101.

Table 4-7 *continued*
Filter Rules

Filter Rule	Description
Report include users	This filter allows you to specify one or more users that you want to be included in the report. The default is "*", which indicates that all users are potentially reported. For instructions, see "Report Include Users" on page 101.

When you create an audit report, AUDITCON applies these filters to records that it reads from the audit file. AUDITCON reports only those events that match all the filter criteria. That is, the audit record timestamp must match the date/time filter and the audit record event type must match the event type filter, and so on. If a filter contains conflicts between "include" and "exclude" options, the "exclude" option takes priority.

4. **When you have finished defining all the filter criteria, return to the "Edit report filter" menu (502) and press** Esc**.**

   AUDITCON asks for confirmation before it saves the filter information.

5. **If you choose "Yes" to save the changes, AUDITCON prompts you for the name of the filter file.**

   The filter name can be up to eight characters long and must not contain a period. AUDITCON appends a ".ARF" extension to the filter name (for example, "FILTER_3.ARF"), and writes the filter file in the auditor's current directory.

Report by Date/Time

Procedure

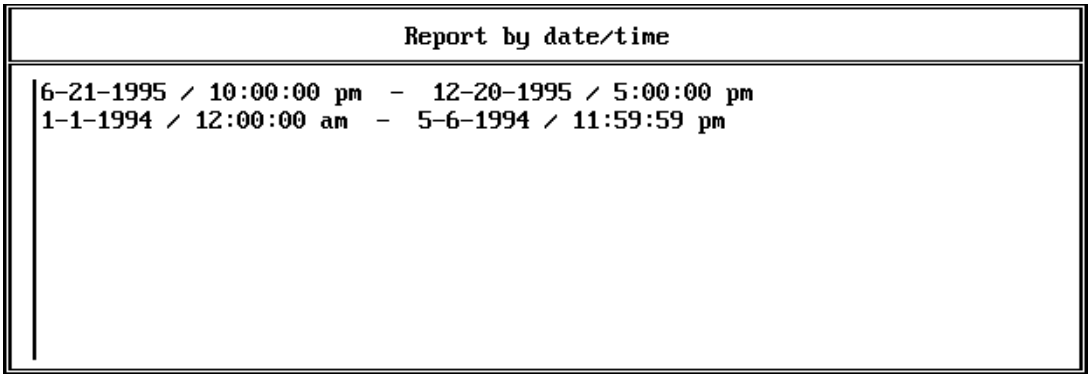
Procedure

1. **From the "Edit report filter" menu, choose "Report by date/time."**

   AUDITCON displays menu 503, which lists the existing date/time ranges defined for the filter.

   If you are inserting a new filter, this menu initially will be empty.

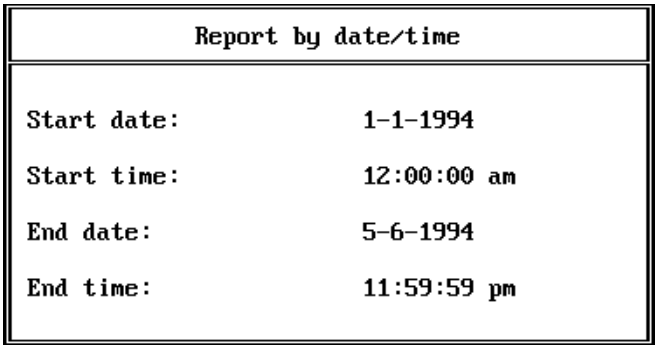
Figure 4-28
Menu 503: Report by Date/Time



2. **Highlight an entry and press** Enter **to edit an existing date/time range, or press** Insert **to define a new range, or highlight an entry and press** Delete **to remove a time range from the filter.**

   If you press Insert or Enter, AUDITCON displays menu 504, which allows you to do more editing of the date/time profile selected in menu 503.

Figure 4-29
Menu 504: Report by Date/Time



3. **To edit the date/time profile, use the arrow keys to move the cursor to the desired field and type in the new value.**

   AUDITCON makes reasonable attempts to convert alternate forms (for example, "3/15/95", "mar 15", "15 Mar 95", "8am", or "8a") into the standard format.

4. **When you have reviewed the date/time range, press** Esc **to return to menu 503.**

5. **Choose "Yes" to save your changes or "No" to cancel the changes.**

   If AUDITCON finds an error (for example, the start date/time later than the end date/time), it displays an error message and goes back to menu 504.

6. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Report by Event

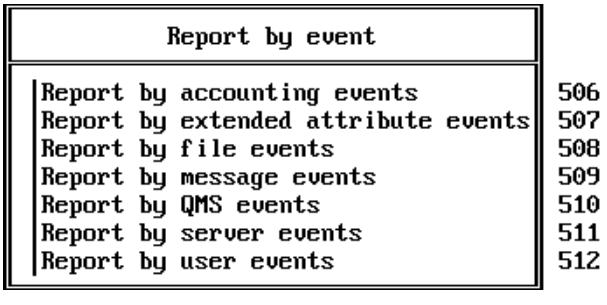
Procedure

Procedure

1. **From the "Edit report filter" menu, choose "Report by event."**

   AUDITCON displays menu 505, which provides a high-level selection of the types of audit events (file system events, queue events, server events, and user events) defined in the current filter.

Figure 4-30
Menu 505: Report by Event



Note

QMS events occur only in the volume SYS: audit trail. If you are examining another volume's audit trail, the menu item identified as 510 will not be present.

2. **Choose one of the types of audit events.**

   See "Audit by Event" on page 50 for descriptions of these events.

   When you choose a type of event, one of the following seven menus will appear.

   Each of the menus has three columns:

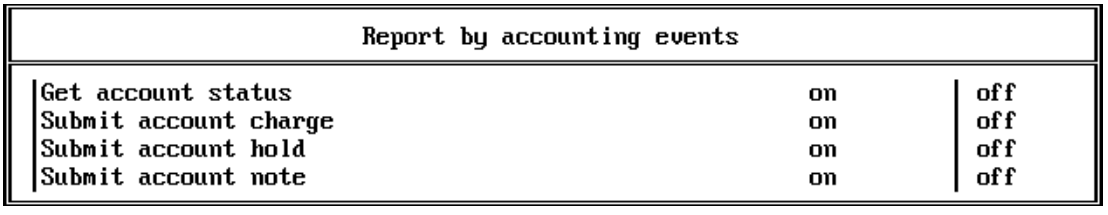
   - An event type (left column)

- An indication of whether the event is preselected for auditing in the current audit file (middle column)
- Flags for toggling the event on or off in the current audit filter (right column)

The preselection indication is with respect to the current configuration of the current audit file, and might bear no significance to the events that are actually recorded in the audit files to which the filter is applied.

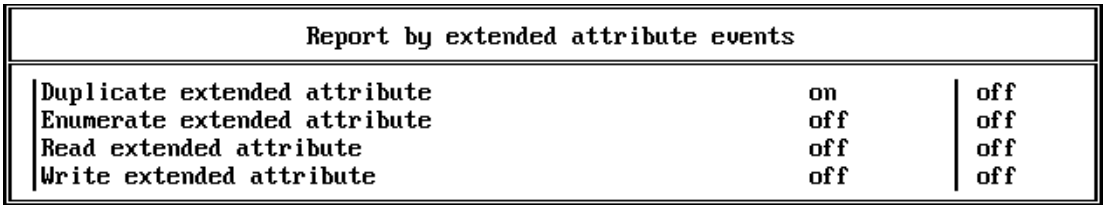
Report by accounting events. This menu shows the accounting audit events that are included in the current filter.

Figure 4-31
Menu 506: Report by Accounting Events



Report by extended attribute events. This menu shows the extended attribute audit events that are included in the current filter.

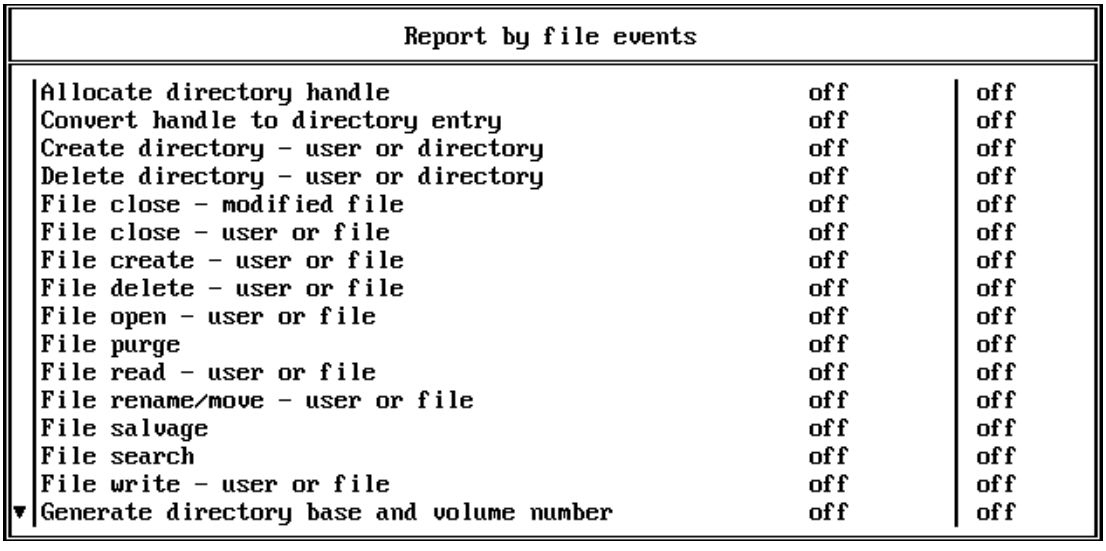
Figure 4-32
Menu 507: Report by Extended Attribute Events



Report by file events. This menu shows the file and directory audit events that are included in the current filter.

Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up and Page Down and arrow keys.

Figure 4-33
Menu 508: Report by File Events



Report by file events

Allocate directory handle	off	off
Convert handle to directory entry	off	off
Create directory - user or directory	off	off
Delete directory - user or directory	off	off
File close - modified file	off	off
File close - user or file	off	off
File create - user or file	off	off
File delete - user or file	off	off
File open - user or file	off	off
File purge	off	off
File read - user or file	off	off
File rename/move - user or file	off	off
File salvage	off	off
File search	off	off
File write - user or file	off	off
Generate directory base and volume number	off	off

The following events can be displayed by scrolling the "Report by file events" screen:

Get entry access rights
Get reference count for directory entry
Get specific information for entry
Get users' effective rights
Lock file
Modify directory entry - user or file
Obtain entry information
Scan deleted files
Scan trustee list
Scan volume's user disk restriction
Search specified directory
Set compressed file size
Set directory handle

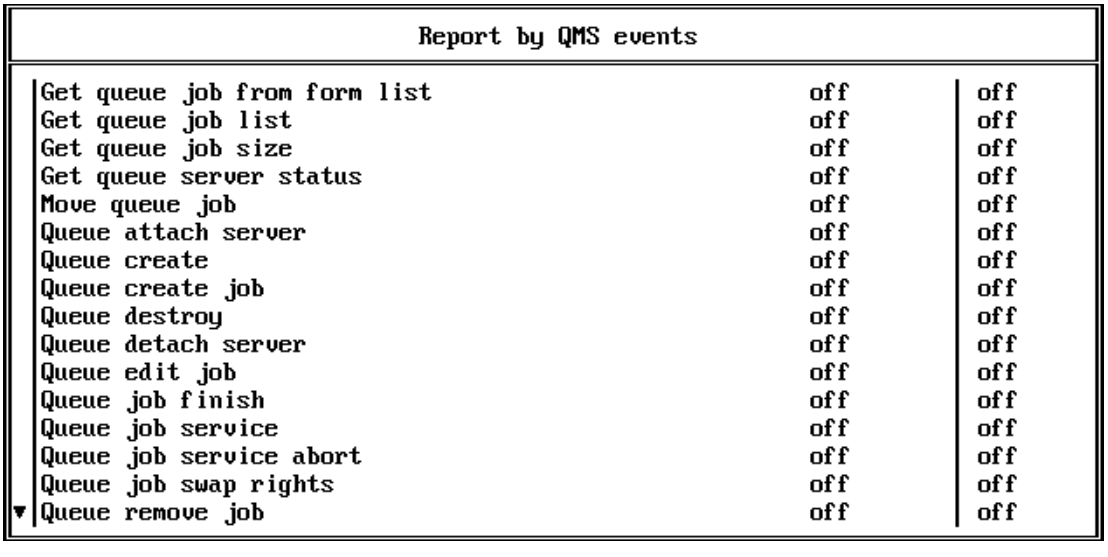
Report by message events. This filter shows the message audit events that are included in the current filter.

Figure 4-34
Menu 509: Report by Message Events

Report by message events		
Broadcast to console	off	off
Disable broadcasts	off	off
Enable broadcasts	off	off
Get broadcast message	off	off
Send broadcast message	off	off

Report by QMS events. This filter shows the print and queue events that are included in the current filter. Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up and Page Down and arrow keys.

Figure 4-35
Menu 510: Report by QMS Events



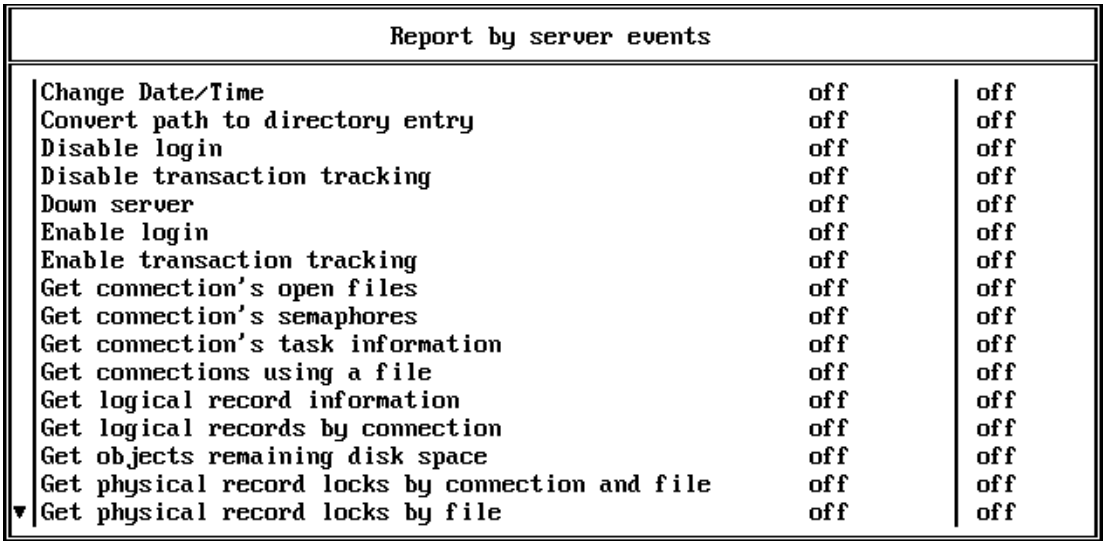
Report by QMS events		
Get queue job from form list	off	off
Get queue job list	off	off
Get queue job size	off	off
Get queue server status	off	off
Move queue job	off	off
Queue attach server	off	off
Queue create	off	off
Queue create job	off	off
Queue destroy	off	off
Queue detach server	off	off
Queue edit job	off	off
Queue job finish	off	off
Queue job service	off	off
Queue job service abort	off	off
Queue job swap rights	off	off
▼ Queue remove job	off	off

The following events can be displayed by scrolling the "Report by QMS events" screen:

Queue set job priority
Queue set status
Queue start job
Read queue job entry
Read queue status
Restore queue server rights
Set print job environment
Set queue server status

Report by server events. This filter shows the server audit events defined for the current menu. Because of the screen size, only 16 events are shown at one time, with the remainder of the events available using the Page Up and Page Down and arrow keys.

Figure 4-36
Menu 511: Report by Server Events



The following events can be displayed by scrolling the “Report by server events” screen:

Get physical record locks by file
Get semaphore information
Get user disk utilization
Map directory number to path
NLM add audit record
NLM add user ID record
Relinquish connection
Remote add name space
Remote dismount volume
Remote execute configuration file
Remote load NLM
Remote mount volume
Remote set console parameters
Remote unload NLM
Send console broadcast
Server console command
Verify server serial number
Volume dismount
Volume mount

Report by user events. This filter lists the user events defined for the current filter.

Figure 4-37
Menu 512: Report by User Events

```
                    Report by user events

Clear connection                          off      off
Disable account                           off      off
Grant trustee                             off      off
Log in user                               on       off
Log out user                              off      off
Remove trustee                            off      off
User space restrictions                   off      off
```

3. **To change preselection of events in the current filter, choose an event and press** F10 **to toggle the setting for that event in the right column.**

4. **When you are finished, press** Esc **to return to menu 505.**

Report Exclude Paths/Files

Procedure

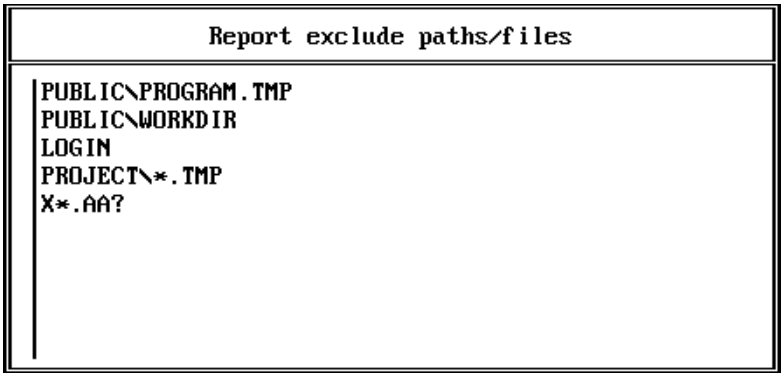
Procedure

1. **From the "Edit report filter" menu, choose "Report exclude paths/files."**

   AUDITCON displays menu 513, which lists the audit filter's pathnames to be excluded from audit reports.

   As shown in the menu, path specifications do not include a volume name or leading backslash, but rather are relative to the root of the volume. Path specifications can contain DOS wildcard characters (* and ?) in the last component of the name.

Figure 4-38
Menu 513: Report Exclude Paths/Files



Warning

AUDITCON does not verify that the paths entered are valid pathname specifications. If they are not valid, they are ignored.

2. **Press** Insert **to define a new pathname. When prompted for the path/filename, press** Enter **to edit an existing entry or press** Delete **to remove an existing entry. Press** Insert **twice to browse the volume files and directories to select pathnames to be excluded.**

3. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Procedure

Procedure

1. **From the "Edit report filter" menu, choose "Report exclude users."**

   AUDITCON displays menu 515, which lists the audit filter's users to be excluded from audit reports.

2. **Press** Insert **to define a new username. When prompted for the username, press** Enter **to edit an existing entry or press** Delete **to remove an existing entry. Press** Insert **twice to browse the list of usernames to select usernames to be excluded from audit reporting.**

   The list of users displayed is those users in the default bindery context for the server where the volume is located.

Warning

The list of users shown is not the complete list of users who might have audit records in the audit file. If you want to exclude users other than those in the default bindery context, you must type their names, rather than selecting them using the browser. Enter the full context without a preceding period (.), such as JOE.SALES.NOVELL.

Note

The status shown in menu 517 for each user is the current status, which is not necessarily the same status of the user when the audit data was recorded.

AUDITCON does not verify that the user names entered are valid. If they are not valid, they are ignored.

Figure 4-39
Menu 515: Report Exclude Users

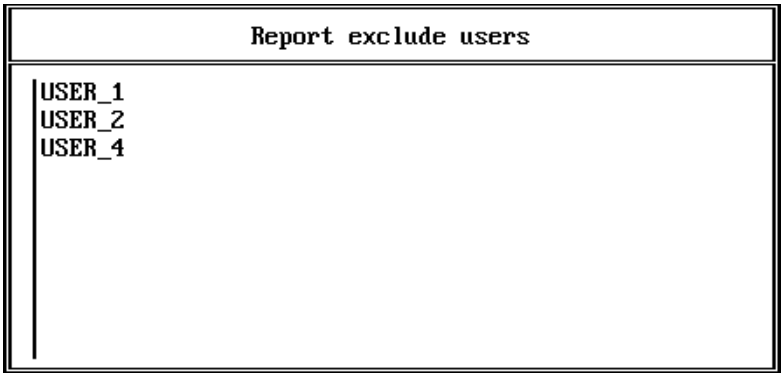
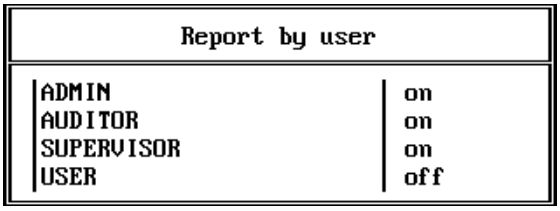


Figure 4-40
Menu 517: Report by User



3. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Report Include Paths/Files

Procedure

Procedure

1. **From the "Edit report filter" menu, choose "Report include paths/files."**

   AUDITCON displays a list of the audit filter's pathnames to be included in audit reports.

   Initially, this screen contains only an asterisk to indicate that all paths / files are to be included in the audit report, but you can edit the menu (as described in "Report Exclude Users" on page 100) to specify a few important pathnames.

2. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Report Include Users

Procedure

Procedure

1. **From the "Edit report filter" menu, choose "Report include users."**

   AUDITCON displays a list of the audit filter's users to be included in audit reports.

   Initially, this screen contains only an asterisk to indicate that all users are to be included in the audit report, but you can edit the menu (as described in "Report Exclude Users" on page 100) to specify a few important users.

2. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Procedure

1. **At menu 501, press** Delete **to remove a selected audit filter.**

   AUDITCON asks for confirmation.

2. **Choose "Yes" and press** Enter **to delete the .ARF file that contains the specified audit filter or "No" to leave the filter in place.**

   AUDITCON displays menu 501, and lists the remaining filters (that is, .ARF files) in the current directory. If you have deleted the last remaining audit filter in the current directory, AUDITCON shows "_no_filter_" in menu 501.

3. **Press** Esc **to return to the "Edit Report Filter" menu (502).**

Report Audit File

This section describes how to generate a formatted text version of the user events in the current audit file. You cannot directly print the server's audit files, because the server's audit files are not directly accessible to network clients and the server's audit files are stored in a compressed format.

Prerequisites

- ❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedure

1. **Choose "Report audit file" from the "Auditing reports" menu (500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

3. **AUDITCON displays menu 526, which shows the available filters. These include the files with .ARF extensions in your current directory and a null filter ("_no_filter_") that will pass all records in the audit file. To use one of these filters, select that filter and press** Enter**.**

Figure 4-41
Menu 526: Select Filter

AUDITCON also allows you to create a temporary filter, or modify an existing filter, for use in this report. Choose the desired filter (or "_no_filter_") and press F10. Edit the filter as described in "Generating Reports from Offline Audit Files" on page 122, then press Esc to bring up the "Save filter" menu. From there you can discard the changes, save the changes to a filter file, or apply the filter to the current report without saving the changes.

4. **AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.**

   Depending on the size of the audit file and the complexity of your filter, this can be a time-consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

5. **To review the contents of your report, exit to DOS and either print or use an editor.**

Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file.

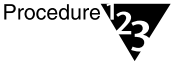
Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 86.

- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures



1. **Choose "Report audit history" from the "Auditing reports" menu (500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

3. **AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file.**

   AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

4. **To review the contents of your report, exit to DOS and either print or use an editor.**

Report Old Audit File

This section describes how to generate a formatted text version of the user events in an old online audit file.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

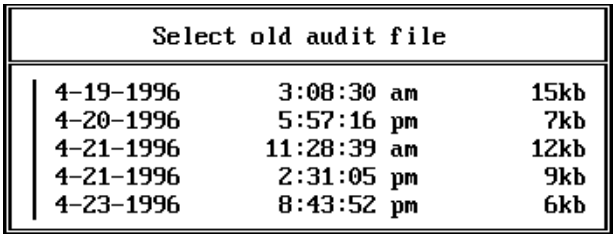
Procedures

Procedure

Choose “Report old audit file” from the “Auditing reports” menu (500).

AUDITCON displays menu 540, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-42
Menu 540: Select Old Audit File



5. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

6. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

7. AUDITCON displays menu 542, which shows the available filters. Choose the desired filter and press Enter**, or press** F10 **to edit a filter.**

Figure 4-43
Menu 542: Select Filter

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.

Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

8. To review the contents of your report, exit to DOS and either print or use an editor.

Report Old Audit History

This section describes how to generate a formatted text version of the auditor events in an old online audit file.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

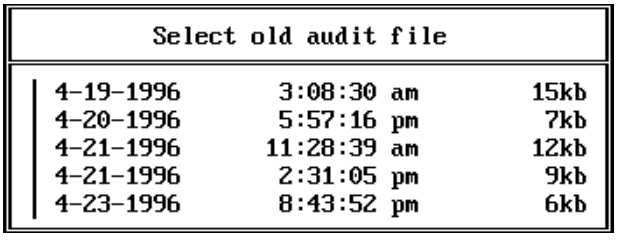
Procedures

Procedure

1. **Choose “Report old audit history” from the “Auditing reports” menu (500).**

   AUDITCON displays menu 550, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-44
Menu 550: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

4. **AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file.**

   AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

5. **To review the contents of your report, exit to DOS and either print or use an editor.**

View Audit File

This section describes how to display a listing of the user events in the current audit file on the screen of your workstation.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 86.

Procedures

1. **Choose "View audit file" from the "Auditing reports" menu (500).**

   AUDITCON displays menu 560 to display the available filters. These include the files with .ARF extensions in your current directory and a null filter ("_no_filter_") that will pass all records in the audit file.

   If AUDITCON does not display the desired filter, return to DOS, change to the directory where the filter is located, and try again.

Figure 4-45
Menu 560: Select Filter

2. Choose the desired filter and press Enter**, or press** F10 **to edit a filter.**

If you select a filter and press Enter, the audit file is displayed. The second line of the header area shows your location in the audit file or when AUDITCON is waiting for information from the server. "-- HOME --" indicates the beginning of the file and "-- END --" indicates the end of the audit file.

Figure 4-46
Sample audit file

```
AUDITCON  4.28                                  Monday  June  10, 1996  3:26pm
 Server: ACME_ONE   Volume: SYS                                  -- HOME --

-- 6-10-1996 --
15:24:00 Start volume audit file, event 80, ACME_ONE_SYS.market.ALPHABET
15:24:00 Active connection, event 58, address 01010340:00001B1E69ED, status 0,
         user ADMIN, connection 19
15:24:22 Get entry access rights, event 213, SYSTEM\TEMP, status 0,
         user ADMIN, connection 19
15:24:22 Set directory handle, event 218, SYSTEM\TEMP, status 0,
         user ADMIN, connection 19
15:24:30 File search, event 219, \, status 255,
         user ADMIN, connection 19
15:24:30 File search, event 219, \, status 255,
         user ADMIN, connection 19
15:24:30 Allocate directory handle, event 217, directory handle 8, SYSTEM\TEMP,
         status 0, user ADMIN, connection 19
15:24:38 Get entry access rights, event 213, SYSTEM, status 0,
         user ADMIN, connection 19
15:24:38 Set directory handle, event 218, SYSTEM, status 0,
         user ADMIN, connection 19
15:24:56 File search, event 219, \, status 255,
         user ADMIN, connection 19
15:24:56 File search, event 219, \, status 255,
```

At any time you can press Home to return to the beginning of the file, or End to go to the end of the file. Press Page Down or Page Up to display a new page of formatted audit records, or use the down or up arrow keys to change the display one record at a time. When AUDITCON is waiting for data from the server, it displays a "-- Reading file --" notification; otherwise, it displays "-- PAUSE --".

AUDITCON displays the time (for example, “17:38:28”) for each audit record, but only displays the date (“-- 3-14-1995 --”) at the beginning of an audit file or when the date rolls over from one day to the next. The first record defines the start time of the audit file and the server / volume being audited.

Subsequent events define the name of the event (for example, “Open file handle”), a numeric event number (“64”), a pathname (“\PUBLIC\AUDITCON.EXE”), the status for the event (in this case, 0 indicates success), the user name, and the user connection number. See Appendix A, “Audit File Formats,” on page 267 for more information on the format of individual events.

If an audit event was generated as a result of an action by a user who was not logged in (typically, by a user reading \LOGIN\LOGIN.EXE), then the username will be _NOT_LOGGED_IN in place of the actual username.

When examining console audit events, you will need the manual console audit log (described in “Maintaining a Console Audit Log” in Chapter 2) to determine the responsible administrator for each action.

3. **Press** Esc **when you are finished.**

   AUDITCON asks for confirmation that you are done.

4. **Choose “Yes” and press** Enter **to return to menu 500.**

View Audit History

This section describes how to display a listing of the auditor events on the screen of your workstation.

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.

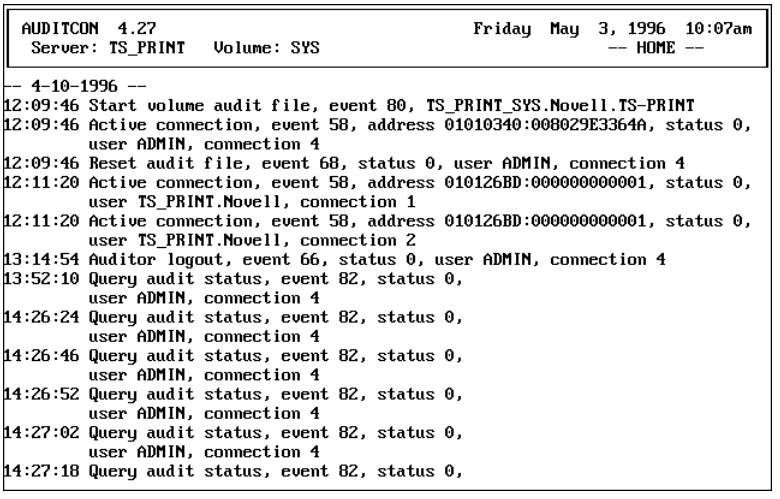
Procedures

Procedure

1. **Choose “View audit history” from the “Auditing reports” menu (500).**

AUDITCON reads the current audit file and displays menu 570, which contains the first screen of audit history events.

Figure 4-47
Menu 570: View Audit History



2. **Press the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer "Yes" to return to menu 500.**

Note

The "Auditor login" event means that an auditor began accessing the audit file, while the "Auditor logout" event means that an auditor ceased accessing the access file. These events do not indicate user logins or logouts.

View Old Audit File

This section describes how to display a listing of the user events from an old online audit file to the screen of your workstation.

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Prerequisites" on page 86.

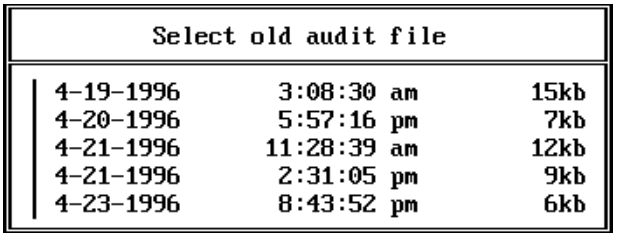
Procedures

Procedure

1. Choose "View old audit file" from the "Auditing reports" menu (500).

AUDITCON displays menu 580, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-48
Menu 580: Select Old Audit File



2. Move the cursor to select the desired audit file, then press Enter**.**

AUDITCON displays menu 581 to display the available filters.

Figure 4-49
Menu 581: Select Filter

3. Choose the desired filter and press Enter**, or press** F10 **to edit a filter.**

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and displays the formatted records to your screen. The screen format is described in "Generating Volume Audit Reports" on page 86.

4. Press the Home**,** End**,** Page Up**,** Page Down**, and** Arrow **keys to move through the display. When you are finished, press** Esc **and answer "Yes" to return to menu 500.**

View Old Audit History

This section describes how to display a listing of the auditor events from an old online audit file to the screen of your workstation.

Prerequisites

Checklist

❑ See“General Prerequisites” on page 29 and “Prerequisites” on page 86.

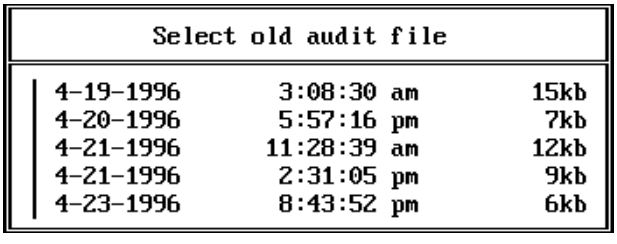
Procedures

Procedure

1. **Choose “View old audit history” from the “Auditing reports” menu (500).**

   AUDITCON displays menu 590, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-50
Menu 590: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON retrieves records from the current audit file, formats the records, and displays them to your screen. The screen format is described in “Generating Volume Audit Reports” on page 86.

3. **Press the** Home**,** End**,** Page Up**,** Page Down**, and** Arrow **keys to move through the display. When you are finished, press** Esc **and answer “Yes” to return to menu 500.**

Database Report Audit File

This section describes how to generate a file containing the user events in the current audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the database file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

Procedure

1. **Choose “Database report audit file” from the “Auditing reports” menu (500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 801 to display the available filters. These include the files with .ARF extensions in your current directory and a null filter (“_no_filter_”) that will pass all records in the audit file.

Figure 4-51
Menu 801: Select Filter

3. **To use one of these filters, choose that filter and press** Enter**.**

AUDITCON also allows you to create a temporary filter, or modify an existing filter, for use in this report. Choose the desired filter (or “_no_filter_”) and press F10. Edit the filter as described in “Generating Reports from Offline Audit Files” on page 122, then press Esc to bring up the “Save Filter” menu. From there you can discard the changes, save the changes to a filter file, or

apply the filter to the current report without saving the changes.

4. **AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.**

   Depending on the size of the audit file and the complexity of your filter, this can be a time-consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

5. **Exit to DOS and use an appropriate database loading program to insert the audit records into a database for review.**

   See "Format of the Database Output File" on page 121 in this chapter for a description of the format of the database file.

Database Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file in a format suitable for loading into a database.

Prerequisites

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

1. **Choose “Database report audit history” from the “Auditing reports” menu (500).**

   AUDITCON prompts you for the name of the output file. Enter the pathname for the file and press Enter.

   AUDITCON attempts to create the file and displays an error screen if it cannot.

   If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

   AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file.

   AUDITCON displays a “Reading file” message in the header area of your screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 500.

2. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

   See “Format of the Database Output File” on page 121 for a description of the format of the database file.

Database Report Old Audit File

This section describes how to generate a file containing the user events in an old online audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

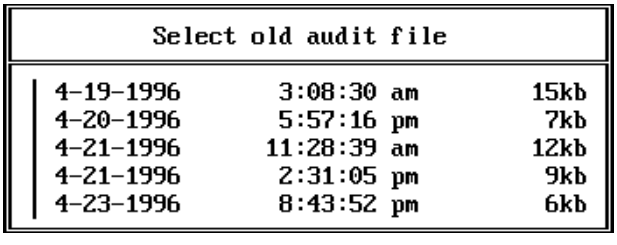
Procedures

Procedure

1. **Choose “Database report old audit file” from the “Auditing reports” menu (500).**

   AUDITCON displays menu 820, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-52
Menu 820: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 822 to display the available filters.

Figure 4-53
Menu 822: Select Filter

4. Choose the desired filter and press Enter**, or press** F10 **to edit a filter.**

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.

Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

5. Exit to DOS and use an appropriate database loading program to insert the audit records into a database for review.

See "Format of the Database Output File" on page 121 for a description of the format of the database file.

Database Report Old Audit History

This section describes how to generate a file containing the auditor events in an old online audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and “Prerequisites” on page 86.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

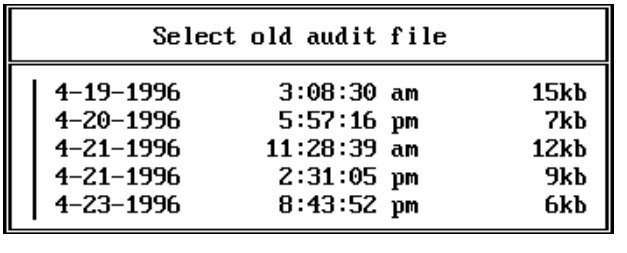
Procedures

Procedure

1. **Choose “Database report old audit history” from the “Auditing reports” menu (500).**

   AUDITCON displays menu 830, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-54
Menu 830: Select Old Audit File



2. **Move the cursor to move the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file.

AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 500.

4. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

See "Format of the Database Output File" on page 121 for a description of the format of the database file.

Format of the Database Output File

Each line in the output file represents a single audit record. Each line consists of a series of comma-separated fields in the following order:

- Time, as hh:mm:ss
- Date, as mm-dd-yyyy
- A "V" to indicate the record came from a volume audit trail
- The name of the volume where the audit record was generated
- A textual description of the event (for example, "File search")
- The word "event" followed by the numerical event number
- The word "status" followed by the status from the event

- The name of the user for whom the event was generated
- Zero or more pieces of event specific information

This format is suitable to be imported into most databases by specifying that the input is a comma-separated text file.

Generating Reports from Offline Audit Files

In addition to processing online audit files (“Generating Volume Audit Reports” on page 86), AUDITCON also allows you to process offline audit files. These offline files can be stored on the auditor’s workstation, removable media, or even in the auditor’s directory on the server file system. Files stored in the server file system are considered offline, even if they contain audit data, because the server does not directly manage these files as audit files.

Offline audit files are in the same compressed, binary format as the server’s audit files described in Appendix A, “Audit File Formats,” on page 267.

This section describes how to process and protect these offline audit files.

Offline Report Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ To process offline audit files, you must either have the Read right to the Audit File object Audit Contents property or have logged in to the audit trail.

AUDITCON controls access to the offline audit file based on the current contents of the Audit File object for that file. Your rights to the Audit File object might be different from your rights when the offline audit file was recorded, so, for example, you might not be able to read an offline audit file that you recorded. This is a constraint imposed by AUDITCON, and not a server access control mechanism. Offline audit files must be protected by the client trusted computing base or (for removable media) by physical protection.

- ❑ You must have previously copied an online audit file from the server to a diskette, your local workstation hard drive, or a network drive. (See “Copy Old Audit File” on page 128 for more information on copying a server's audit files.)

- ❑ You must have access to an offline audit file. You must have at least Read and File Scan rights to access offline audit files on network drives. See your workstation documentation for information on using file system rights on your workstation.

Procedures

Procedure

1. **Choose "Reports from old offline file" from the "Available audit options" menu (101).**

   AUDITCON prompts you for the name of an offline audit file.

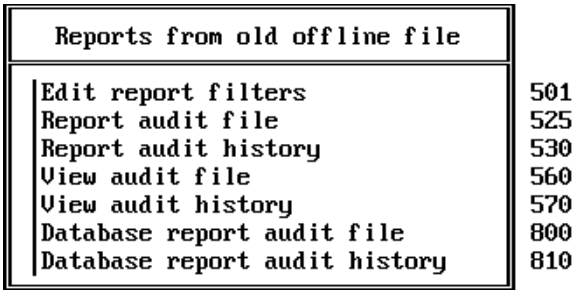
   For DOS workstations, the filename can be an absolute DOS pathname (for example, "F:\AUDIT\95FEB15.DAT") or a relative pathname in your current directory (for example, "AUDIT.DAT").

2. **Enter the pathname for the offline audit file. Press** Enter **to open the audit file, or** Esc **to return to menu 600.**

   If AUDITCON cannot open the file, it displays an error message.

3. **If AUDITCON can open the file, it displays menu 602, which permits you to choose more operations on the offline audit file.**

Figure 4-55
Menu 602: Reports from Old Offline File



4. **Choose the desired operation, then press** Enter **to perform that operation.**

Edit Report Filters

This section describes how to create and edit report filters that you can use to display specific information that is of interest. There is no

distinction between filters for online files and filters for offline files; if you've already created a filter for viewing online audit files, you can use (or modify) that filter for viewing offline audit files.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Offline Report Prerequisites" on page 122.

Procedures

1. **Choose "Edit report filters" from the "Reports from old offline files" menu (602).**

   AUDITCON displays menu 501.

2. **Follow the procedures in "Edit Report Filters" on page 88 to create or edit audit report filters.**

Report Audit File

This section describes how to generate a formatted report of the audit records in an offline audit file.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Offline Report Prerequisites" on page 122.

Procedures

1. **Choose "Report audit file" from the "Reports from old offline files" menu (602).**

   AUDITCON displays menu 525.

2. **Follow the procedures in "Edit Report Filters" on page 88 to generate an audit report for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Report Audit History

This section describes how you can generate an text report of the audit history information in an offline audit file.

Prerequisites

❑ See “General Prerequisites” on page 29 and the “Offline Report Prerequisites” on page 122.

Procedures

1. **Choose “Report audit history” from the “Reports from old offline files” menu (602).**

   AUDITCON displays menu 530.

2. **Follow the procedures in “Report Audit History” on page 104 to generate a text audit history report for an offline audit file.**

   References in that section to the “current audit file” should be interpreted as references to an offline audit file.

View Audit File

This section describes how you can view (on your workstation screen) audit records from an offline audit file.

Prerequisites

❑ See “General Prerequisites” on page 29 and “Offline Report Prerequisites” on page 122.

Procedures

1. **Choose “View audit file” from the “Reports from old offline files” menu (602).**

   AUDITCON displays menu 560.

2. **Follow the procedures in “View Audit File” on page 109 to view an offline audit file.**

References in that section to the “current audit file” should be interpreted as references to an offline audit file.

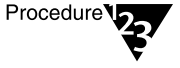
View Audit History

This section describes how you can view (on your workstation screen) the audit history for an offline audit file.

Prerequisites

❑ See “General Prerequisites” on page 29 and “Offline Report Prerequisites” on page 122.

Procedures



1. **Choose “View audit history” from the “Reports from old offline files” menu (602).**

   AUDITCON displays menu 570.

2. **Follow the procedures in “View Audit History” on page 111 to view the audit history for an offline audit file.**

   References in that section to the “current audit file” should be interpreted as references to an offline audit file.

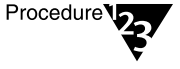
Database Report Audit File

This section describes how to generate a report of the audit records in an offline audit file in a form suitable for loading into a database.

Prerequisites

❑ See “General Prerequisites” on page 29 and “Offline Report Prerequisites” on page 122.

Procedures



1. **Choose “Database report audit file” from the “Reports from old offline files” menu (602).**

   AUDITCON displays menu 800.

2. **Follow the procedures in "Database Report Audit File" on page 114 to generate an audit report for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Database Report Audit History

This section describes how you can generate a report of the audit history information in an offline audit file in a form suitable for loading into a database.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Offline Report Prerequisites" on page 122.

Procedures

1. **Choose "Database report audit history" from the "Reports from old offline files" menu (602).**

   AUDITCON displays menu 810.

2. **Follow the procedures in "Database Report Audit History" on page 117 to generate a text audit history report for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Volume Audit File Maintenance

This section describes how you can use AUDITCON to close, copy, delete, and display the server's old audit files. These mechanisms work only for old audit files, that is, the files maintained online by the server.

You cannot perform these operations on offline audit data files. The only operation you can perform on the server's current audit file is to reset the file, which causes the server to roll over to a new current audit file.

Audit File Maintenance Prerequisites:

Checklist

❑ See “General Prerequisites” on page 29.

Procedures

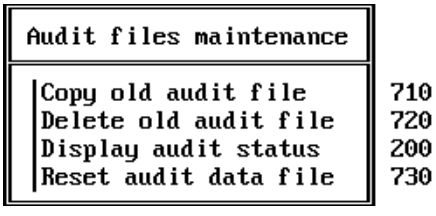
Procedure

1. **Choose “Audit files maintenance” from the “Available audit options” menu (101).**

2. **Press** Enter**.**

   AUDITCON displays menu 700, which lists more maintenance options.

Figure 4-56
Menu 700: Audit Files Maintenance



Copy Old Audit File

This section describes how to copy old online audit files to removable media (for example, diskettes or magnetic tapes), workstation directories, or network drives. The primary reason for copying an audit file is to save the contents of the file before you delete it from the server (see “Delete Old Audit File” on page 131). You might also want to copy an old audit file to removable media in order to save it for evidence or to keep it for long-term storage.

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29.

❑ To copy an online audit file, you must either have Read rights to the Audit File object Audit Contents property or have logged in to the audit trail. (To log in to an audit trail, you must enable audit passwords at the server console; this configuration is not permitted in trusted facilities.)

- ❑ You must have sufficient rights on your workstation or network drive in order to copy the audit file to that directory. For network drives, you must have at least the Create right. See your client documentation for more information on rights required to create a file on a hard drive or diskette.

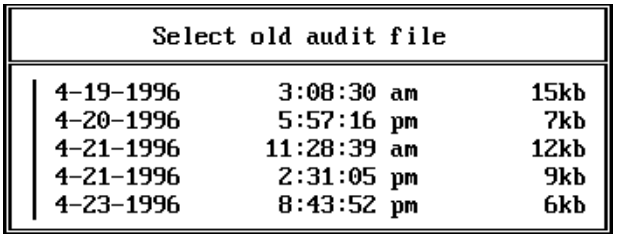
Procedure

Procedure

1. Choose “Copy old audit file” from the “Audit files maintenance” menu (700).

AUDITCON displays menu 710, which lists up to 15 old audit files that are maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-57
Menu 710: Select Old Audit file



Note

There is no mechanism for copying the contents of the current audit file. If you want to copy this data, you must first reset the audit data file as described in “Reset Audit Data File” on page 132.

You can only copy one file at a time. If you want to copy multiple audit files, perform the steps in this section once for each file.

2. Move the cursor to choose the desired audit file, then press Enter**.**

AUDITCON prompts you for the name of the offline audit file.

3. Enter the filename of the destination audit file and press Enter**.**

The pathname must be a DOS pathname on your local workstation, for example, “A:\AUDIT301.DAT”, “C:\AUDIT\FILE1.DAT”, or “F:\AUDITOR\VOL1\A950224.DAT”.

If you do not specify a drive letter and directory, AUDITCON leaves the audit file in your current directory. The default filename is "AUDITOLD.DAT" on your local drive.

AUDITCON displays a "Please wait" message while it copies the audit file from the server to your offline destination file. When it has copied the file, AUDITCON returns to menu 700.

4. **If you copy audit files from the server onto your local workstation's file system, you must ensure that the audit data is properly protected by your workstation.**

5. **If you copy the audit file onto removable media (for example, a diskette or tape cartridge), attach a diskette or tape label that shows the server name, volume name, your name, the date, time, and size of the audit file, along with any other specific comments that you feel are important. Finally, you must ensure that the media is physically protected.**

   The purpose of this information is to ensure that you can load the medium in the future, and generate meaningful audit reports from it.

One strategy that is commonly used is to set the maximum audit file size so that one audit file will fit on a 1.44 MB diskette. See "Changing a Volume Audit Configuration" in this chapter for information on setting the audit file size.

If you have a high volume of audit data, you will probably want to archive your audit files onto magnetic tape, for example, tape cartridges. AUDITCON does not provide a means for copying audit files directly to magnetic tape. If you want to use magnetic tape for long-term storage, you must first copy those files onto your file system, then use a backup program to copy the files to magnetic tape.

The frequency at which you should copy the server's audit files to offline storage depends on how fast your server fills up audit files. If your server archives audit files on a periodic basis (as opposed to filling up the audit file), then you can set the number of audit files to 10 or 15, and copy or remove online audit files once per week without expecting to overflow the number of audit files.

Delete Old Audit File

This section describes how to delete an old audit file from the server's online storage after you've copied the file to offline storage or decided that you do not need to save the file.

Prerequisites

Checklist

- ❑ See "General Prerequisites" on page 29.
- ❑ To delete an online audit file, you must either have the Write right to the Audit File object Audit Policy property or have logged in to the audit trail. If dual-level passwords are enabled, you must have the level 2 password.

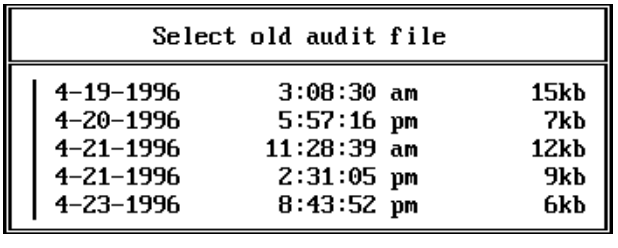
Procedure

Procedure

1. **Choose "Delete old audit file" from the "Audit files maintenance" menu (700).**

   AUDITCON displays menu 720, which lists up to 15 old audit files that are maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 4-58
Menu 720: Select Old Audit File



Note

There is no mechanism for deleting the current audit file. If you want to delete the data in the current audit file, you must first reset the audit data file (see "Reset Audit Data File" on page 132).

You can only delete one file at a time. If you want to delete multiple audit files, perform the steps in this section once for each file.

2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON asks you to confirm that you want to delete the audit file.

After you delete an online audit file, there is no way to recover the contents of the file. Do not delete the file unless you are absolutely certain that you will not require the data in the audit file. If there is any doubt, copy the audit file (see "Copy Old Audit File" on page 128) to offline storage before you delete the file.

3. **If you are certain that you want to delete the old audit file, press** Enter**.**

Reset Audit Data File

This section describes how to reset the current audit file. Resetting a file is a manual means of causing the current audit file to "roll over," that is, to cause the current audit file to become an old audit file and to establish a new current audit file.

Manual reset might be necessary, for example, if the server stops processing volume requests because the volume is in an overflow state. See "Resolving Volume Audit Problems" on page 133 for information on recovering from volume overflow.

Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ To reset the current audit file, you must either have the Write right to the Audit File object Audit Policy property or have logged in to the audit trail. If dual-level passwords are enabled, you must have the level 2 password.

Procedures

1. **Choose "Reset audit data file" from the "Audit files maintenance" menu (700).**

   AUDITCON requests confirmation that you want to perform the reset.

   If you perform the reset, the current audit file will become an old audit file and a new current audit file will be created.

2. **Choose "Yes" and press** Enter **to reset the current volume audit file.**

Resolving Volume Audit Problems

This section describes solutions to potential volume audit problems. These include audit trail overflow and catastrophic failure.

Audit Trail Overflow

"Preventing Loss of Audit Data" on page 23 describes the potential for audit loss if the configured number of audit files are filled or disk space fills up and the audit trail is improperly configured.

"Audit Options Configuration" on page 70 describes the three overflow configuration options for volume audit trails:

- Archive audit file
- Disable auditable events
- Disable event recording

The only option that prevents the loss of audit events (from audit overflow situations) is to disable auditable events. With this setting, the server goes into an overflow state when the current audit file reaches its maximum size or the server cannot write the current audit event.

To recover from this overflow state, an auditor (with the Write right to the volume Audit File object Audit Policy property) must reset the current audit trail.

1. If volume SYS: overflows, the server will allow an auditor to perform a read-only login to reset the audit file.

To perform a read-only login when volume SYS: has overflowed, you must have sufficient software in your workstation to perform the login without downloading anything from the \LOGIN directory. The specific software this requires depends on your workstation.

In general, having a copy of the contents of \LOGIN will be sufficient. To do this, create a \LOGIN directory on your workstation, and copy everything from SYS:\LOGIN to your workstation \LOGIN directory. The required contents include not only the \LOGIN directory itself, but also subdirectories of \LOGIN (that is, \LOGIN\NLS and \LOGIN\NLS\ENGLISH).

If you don't keep a copy of \LOGIN on a workstation, you will be unable to recover from an audit overflow on the SYS: volume.

When in the overflow state, you can log in using your local copy of \LOGIN by changing to that directory and running LOGIN.EXE (or any other appropriate programs).

2. If you want to save the oldest audit file, and you haven't already backed it up, copy the oldest old audit file to offline storage (for example, a file in the server or workstation or removable media).

3. Reset the current volume audit file, as described in "Reset Audit Data File" on page 132. This rolls over the current audit file (to an old audit file), deleting the oldest old audit file, and initializes a new audit file.

4. If you want to save any audit files that you haven't already saved (including the newest of the old audit files), copy those audit files to offline storage.

Perform the following suggestions to help prevent volume overflow:

1. Review the status and size of the audit file frequently.

2. Manually reset the audit file before it overflows, if necessary.

3. Enable "Automatic audit file archiving" as described in "Changing a Volume Audit Configuration" on page 47. Set the "Audit file maximum size" large enough and the "Days between audit archives" low enough that the audit file will not overflow. Use caution in setting these parameters to prevent destruction of audit data.

4. Don't over audit.

If the audit trail for a volume is full, the auditor's actions (for example, deleting data files, resetting the audit file) cannot be audited for that volume. In this case, you must keep a manual log of your actions for use when generating a complete history of actions performed on the server. You will be informed via a message from the server to your workstation when this occurs.

When the audit trail is reaches its configured threshold, you will receive the following notification on your workstation screen:

```
The audit overflow file for volume volname is almost
full.  Auditors must begin manual auditing now!
```

When the audit trail is completely full, you will receive the following notification on your workstation screen:

```
The audit overflow file for volume volname is full.
```

To avoid missing this message, you must not issue the SEND /A=N or SEND /A=P commands, or if using Windows and the NetWare User Tools, do not disable network warnings.

Catastrophic Failure Recovery

This section describes what to do if you have a catastrophic failure, for example, the volume being audited is destroyed (perhaps because of a hard disk failure) and you need to recover the audit state to what it was before the failure. In addition, it explains how to handle planned upgrades, such as when a volume is moved from a small disk drive to a larger disk drive.

There are several potential losses not addressed here:

- Loss of offline audit data. Your offline audit data (whether stored in server or workstation file systems, or on removable media) should be backed up frequently enough that its loss would not be catastrophic.

- Loss of some, but not all copies of the Audit File object describing the volume audit trail due to failure of one or more servers holding an NDS partition. In this case, NDS automatically uses whatever copies are available. If a server configured for the partition is brought back online, then it will automatically be updated with the Audit File object information.

There are two major catastrophic failures possible for volume audit:

- Loss of all copies of the Audit File object describing the volume audit trail. If all copies of the Audit File object are lost (for example, because there only was one copy, and the server it was on suffered a disk failure), then you might be able to recover the Audit File object from a backup of your Directory tree (presuming you have backed up your Directory tree). If so, then you will be able to regain access to the existing online audit data. If not, then no access is possible to the online audit data. You must recreate the volume audit trail using the procedures in “Enabling Volume

Auditing" on page 44 (including selecting events, audit full actions, and so on).

- Loss of a volume (for example, because of a disk failure). Because volume audit files are stored in an inaccessible directory which cannot be backed up, loss of a volume means that the online audit files (both the current audit file and any old audit files) are lost. Use AUDITCON to perform regular backups of audit data to avoid loss of online audit data.

If you restore a volume from a backup, it will come back without auditing enabled. To avoid unaudited actions while you are configuring the audit system, you should take the server offline for the restoration process until the volume audit has been reconfigured. To do this, disconnect the server from any networks it is connected to, and attach it to a protected LAN containing only a trusted workstation located in a secure location. Then restore the volume from the backup. Use the trusted workstation to run AUDITCON to re-enable volume auditing. Restore the previous configuration, using your manual logs of which files are audited (as described in "Changing a Volume Audit Configuration" on page 47). Finally, reconnect the server to the standard networks.

You might need to take more than one server offline to perform this restoration, for example, if the server being restored does not have replicas of any NDS containers with administrative users, or if the Audit File object for the volume audit trail will not be stored in a container found on the server.

In addition to the above scenarios, if you restore an NDS User object from an NDS backup, it will come back without its per-user audit flag. To prevent a user from performing unaudited actions, you should take the server offline before restoring the User object, and use AUDITCON to set the per-user audit flag using the manual logs of audited users (as described in "Audit by User" on page 67 or "Audit by User" on page 161).

If you upgrade a volume (for example, replacing it with a larger disk), that is equivalent to recovery from a catastrophic disk failure. To do an upgrade, you must first back up the old volume, and then restore it on the new disk. This loses all audit data. Therefore, before performing a volume upgrade, you should also back up all volume audit data stored on that server. Because the backup does not include the per-file audit flags, you should use the procedure described above to take the server offline for the recovery process, and use the manual logs of which files are audited to configure the audit system correctly before bringing the server back online.

Immediacy of Changes

When you modify the volume audit trail configuration (for example, to change the maximum size of the audit file or the set of events to be recorded), the change is made both to the Audit Policy property of the Audit File object and to the header of the current audit file.

Both changes will usually occur immediately. However, the effect of the change might not be immediate if the server holding the audit data is unavailable to receive the configuration change (for example, because it is down or the network has been split), even though the Audit File object can be modified. In this case, the delay will depend on how long it takes for the two servers to synchronize their NDS replicas. See *NetWare Enhanced Security Administration* for information on how to determine when synchronization occurs.

In addition, if an auditor is performing audit trail management functions, changing the ACL will not affect the auditor's capabilities (either to increase or decrease them). An auditor's rights are recalculated every time he or she restarts AUDITCON and establishes access to an audit trail. To stop the auditor's actions immediately, you should break the auditor's connection to the server using the console MONITOR utility or the CLEAR STATION console command.

chapter 5

Using AUDITCON for Container Auditing

Guide to NetWare 4 Networks gives an overview of the NDS™ Directory database. It explains that the Directory database is a hierarchical database, consisting of container objects (which contain other objects) and leaf objects (which do not contain other objects).

Container objects can contain any combination of leaf and container objects. You can use various utilities (including AUDITCON) to browse the Directory database for container objects.

NetWare® Enhanced Security provides NDS auditing at the container level; that is, you can enable or disable auditing or set other configuration parameters for an individual container.

As described in Chapter 1, auditing a container records information about attempted accesses to objects (and their properties) located directly in that container. Container auditing doesn't provide audit coverage for objects contained in subcontainers of the audited container.

As described in Chapter 2, the server provides two mechanisms for controlling access to container audit trails

- By assigning NDS rights on the audit trail Audit File object and its object properties
- By assigning a password to the audit trail

Even though the password-based mechanism is not permitted in NetWare Enhanced Security configurations, it is still used by the server and, consequently, is described in this section.

Container auditing is used to audit actions occurring to NDS objects. If you have containers ENGR and FINANCE, where actions in ENGR are audited and actions in FINANCE are not audited, then

- A request by an object in ENGR (for example, a User object) to access an object in ENGR is auditable (depending on whether the particular event has been selected).
- A request by an object in ENGR (for example, a User object) to access an object in FINANCE is not auditable, because access to objects in FINANCE is not audited.
- A request by an object in FINANCE (for example, a User object) to access an object in ENGR is auditable (depending on whether the particular event has been selected).
- A request by an object in FINANCE (for example, a User object) to access an object in FINANCE is not auditable, because access to objects in FINANCE is not audited.

The following topics are described in this chapter.

Accessing the Container Audit Trail

This section describes how to

- Access the container auditing menu tree
- Select a container for auditing
- Log in to a container audit trail (if audit passwords are enabled)

You should have read Chapter 3, which describes how to run AUDITCON and navigate the menu tree.

Getting Started

When you run AUDITCON, it displays a screen with one of the five "Available audit options" menus. The particular entry menu you see depends on your current volume and the state of that volume audit trail.

The container auditing state is independent of the state of volume auditing. You do not have to enable auditing of a volume or have access to a volume audit trail to perform container auditing.

Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ If you are unfamiliar with NDS concepts, review the *Guide to NetWare 4 Networks*. If you are unfamiliar with the implementation of your Directory tree, run a graphical utility such as NetWare Administrator to browse the tree.

See your client documentation for information on the availability of NetWare Administrator or NETADMIN in your client evaluated configuration.

Procedures

Procedure

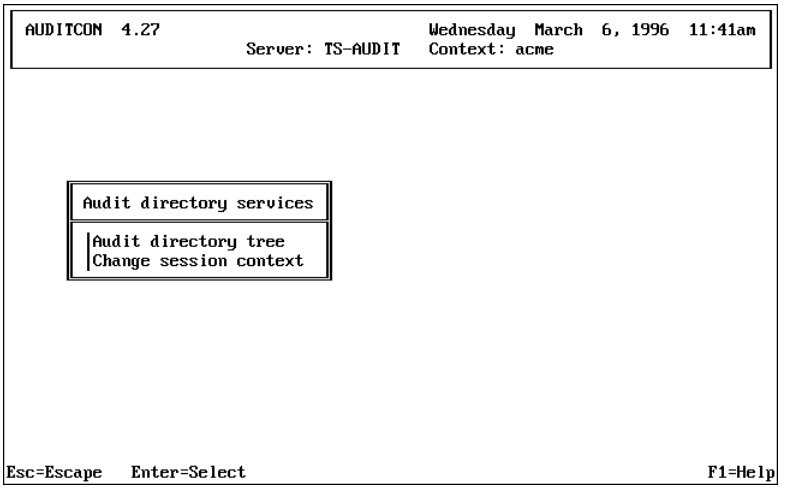
1. **Choose “Audit directory services” from the initial “Available audit options” menu (101, 102, or 103).**

2. **Press** Enter.

   AUDITCON displays menu 1000, which shows the full screen for container auditing. The second line of the header defines your current container (in Figure 5-1, the Organization O=ACME) and the server currently in use (in Figure 5-1, SERVER1).

   As you move from one container to another in the Directory tree, this field shows your current context. In addition, it shows which server is being used for accessing the container audit trail.

Figure 5-1
Menu 1000: AUDITCON Full Screen for Container Auditing



Change Session Context

To audit a container, your session context (shown in the second line of the header area) must point to that container. If not, you must change your session context before you can begin auditing that container.

AUDITCON provides two methods of changing your context. You can type in the explicit context for the container you want to audit, as explained in this section (this might be the preferred method if your network has many containers and you know which container you want to audit).

You can also browse through the Directory tree and select a container for auditing (see "Audit the Directory Tree" on page 144). This is generally the preferred method, because you can select a container and begin auditing that container in a single operation.

You don't need rights to the container or to the container's Audit File object to set the container context.

Prerequisites

❑ See "General Prerequisites" on page 29.

Procedures

1. **To define a different container for auditing, choose "Change session context" in the "Audit directory services" menu (1000) and press** Enter**.**

   AUDITCON displays the "Edit Session Context", which allows you to edit the current session context.

2. **Edit the current session context by backspacing and typing over the existing container name or pressing Home and inserting text at the beginning of the line.**

3. **When you are done, press** Enter **to change context to the specified container.**

   If the container exists, AUDITCON changes your NDS context, updates the context field in the display header area, and returns to menu 1000.

If auditing is enabled, your first selection from the top level menu should be "Change replica" (see "Change Replica" on page 148), to determine

which replica of the partition will be used for auditing. Failure to use the primary copy (as described in “Configuring Auditing” on page 155 and “Container Audit File Maintenance” on page 210) for configuration changes can cause the audit configuration changes to be lost. When doing audit reporting, you should examine each replica of the partition in turn, as described in “Generating Container Audit Reports” on page 172.

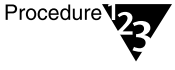
Audit the Directory Tree

This option allows you to browse the Directory tree to select a container for auditing. AUDITCON displays a menu that allows you to begin auditing that container. If you have already selected the container, as described in “Change Session Context” on page 143, you do not need to browse the tree.

Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ To browse the Directory tree for containers, you must have the Browse right to the container. Otherwise, AUDITCON will not be able to find the container.

Procedures

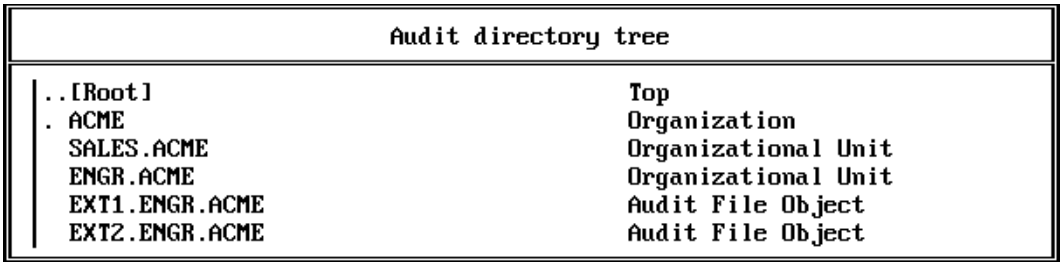


1. **Choose “Audit Directory tree” in the “Audit Directory services” menu (1000) and press** Enter**.**

   AUDITCON displays menu 1010, which allows you to browse the Directory tree to select a container for auditing.

If auditing is enabled, your first selection from the top level menu should be “Change replica” (see “Change Replica” on page 148), to determine which replica of the partition will be used for auditing. Failure to use the primary copy (as described in “Configuring Auditing” on page 155 and “Container Audit File Maintenance” on page 210) for configuration changes can cause the audit configuration changes to be lost. When doing audit reporting, you should examine each replica of the partition in turn, as described in “Generating Container Audit Reports” on page 172.

Figure 5-2
Menu 1010: Audit Directory Tree

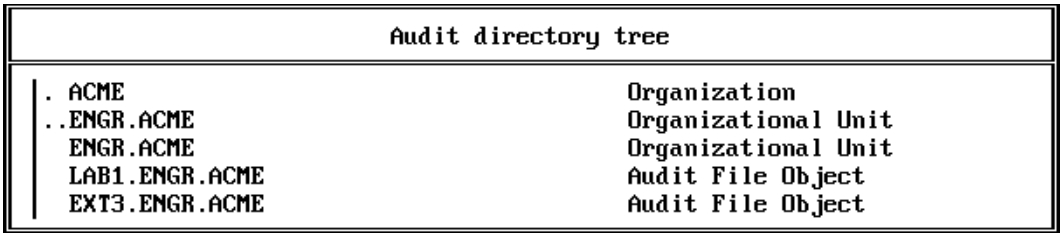


AUDITCON displays the parent of the current container (in this case, "[Root]", indicated by ".."), the current container (in this case, "ACME", indicated by "."), and any containers within the current container (in this case, "SALES.ACME" and "ENGR.ACME").

2. **If the menu does not show the container you want to audit, keep choosing the nearest ancestor and pressing** Enter **until AUDITCON shows the desired container.**

   For example, if you want to audit "LAB1.ENGR.ACME", which is not shown in menu 1010, you would first choose "ENGR.ACME". AUDITCON changes the session context and displays menu 1010-Updated.

Figure 5-3
Menu 1010-Updated: Audit Directory Tree



3. **When the menu shows the desired container, move the cursor to that container. Press** F10 **to review the container audit trail.**

   AUDITCON will change your NDS context and update the context field in the display header area. It will then display one of the top-level menus (see "Top-Level Menus" on page 146).

If you press Enter instead of F10, AUDITCON displays menu 1010 with the new session context, and you can then select the current container for auditing.

Top-Level Menus

After you've selected a specific container for auditing, there are four different top-level menus. AUDITCON selects which menu to display depending upon three variables:

- The setting of the "Allow Audit Passwords" console parameter (which must be set to OFF in the NetWare Enhanced Security configurations)
- Whether you have sufficient rights, defined as either
  - An Audit File object exists for the currently selected container, and you have at least Read or Write rights to the Audit Contents or Audit Policy attribute of the Audit File object
  - An Audit File object does not exist for the currently selected container, but you have sufficient rights to create an Audit File object in the container
- Whether auditing is enabled for the container

Table 5-1, " Container Auditing Entry Menus", summarizes the algorithm AUDITCON uses to determine which menu to display.

Table 5-1
Container Auditing Entry Menus

Allow Audit Passwords = ON	Sufficient Rights	Container Audit Enabled	Menu
Yes	*Yes*	*Yes*	*1101*
Yes	*Yes*	*No*	*1102*
Yes	*No*	*Yes*	*1103*
Yes	*No*	*No*	*1102*
No	Yes	Yes	1101

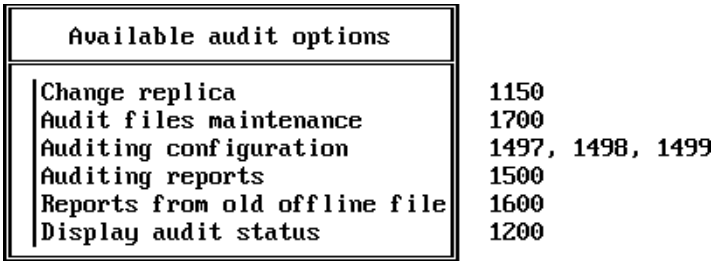
Table 5-1 *continued*
Container Auditing Entry Menus

Allow Audit Passwords = ON	Sufficient Rights	Container Audit Enabled	Menu
No	Yes	No	1102
No	No	Yes	1104
No	No	No	1104

The four top-level "Available audit options" menus for container auditing are as follows:

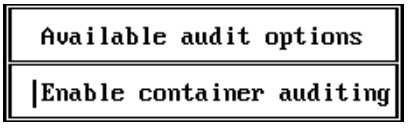
Menu 1101. AUDITCON displays this menu when the auditor has NDS access to the selected container audit trail or has successfully logged in to the audit trail. (outside the NetWare Enhanced Security configurations)

Figure 5-4
Menu 1101: Available Audit Options



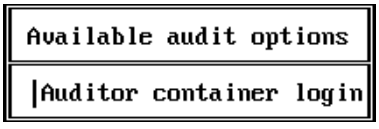
Menu 1102. AUDITCON displays this menu when the selected container is not enabled for auditing.

Figure 5-5
Menu 1102: Available Audit Options



Menu 1103. This is the AUDITCON entry menu when the current container is enabled for auditing but you do not have rights to read or enable the audit trail. If password-based access is permitted for the audit trail (that is, the server console parameter ALLOW AUDIT PASSWORDS is ON), you can select the "Auditor container login" entry and try to log in to the audit trail as described in "Auditor Container Login" on page 149.

Figure 5-6
Menu 1103: Available Audit Options



If you don't have rights to access the audit trail, AUDITCON displays an error message.

Change Replica

This section describes how you can use AUDITCON to select which replica of a container you want to use. This is used for two purposes: to select the replica that you use for all configuration changes, and to select the replica when you are reviewing audit trails (to ensure that you see all audit data by reviewing the data stored in each replica).

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29.

Procedures

Procedure

1. **Choose "Change replica" from the "Available audit options" menu (1101).**

   AUDITCON displays menu 1150, which allows you to choose the server you want to use.

Figure 5-7
Menu 1105: Replicas Stored on Server

Replicas stored on server	Type
BRUTUS.ACME	Master
SERVER_2.ACME	Read/Write
SERVERQ.FINANCE.ACME	Read-Only

2. **Move the cursor to the server name and press** F10 **or** Enter **to choose the server.**

   AUDITCON updates the server name at the top of the screen and returns to menu 1101.

Audit data is stored on master, read/write, and read-only replicas of the container.

Auditor Container Login

Logging in to an audit trail is fundamentally different from logging in to a NetWare Enhanced Security server. When you log in to a NetWare Enhanced Security server, your login password is used to authenticate your individual identity to NDS for the life of your login session. "Logging in" to a container audit trail is a means of controlling access to an audit file, and is not permitted in the NetWare Enhanced Security configuration. However, if you use audit passwords to control access to the audit trail, do not reuse your NetWare login password.

Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ The ALLOW AUDIT PASSWORDS console parameter must be ON at the particular server you are accessing for you to log in to a container audit trail anywhere on that server.

The server's NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. Do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console) because this violates the assumptions under which the server was evaluated. See preceding note under "Change Replica" for additional information.

Procedures

1. **Choose "Auditor container login" in the "Available audit options" menu and press** Enter**.**
2. **Enter the container audit password (after the colon prompt) and press** Enter **to log in to the current container's audit trail.**

   AUDITCON does not echo your password to the screen. If your login is successful, AUDITCON goes to menu 1101.

   If you use the wrong password or audit passwords are disabled for your current server, AUDITCON displays an error report as shown in menu 131. Because password-based access to audit trails

is not permitted in NetWare Enhanced Security configurations (ALLOW AUDIT PASSWORDS is OFF), entry of a container password in a NetWare Enhanced Security configuration will always fail.

3. **Press** Enter **to return to menu 1101.**

   If you are unable to log in to the audit trail, and do not have rights to the container Audit File object, ask your system administrator for help.

Displaying Container Audit Status

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29.
- ❑ To display the container audit status, you must have Read or Write rights to the Audit File object Audit Policy property, or Read or Write rights to the Audit File object Audit Contents property, or have logged in with a level 1 password. See “Controlling Access to Online Audit Data” on page 17 for information about password levels.

Procedures

Procedure

1. **Choose “Display audit status” in menu 1101.**

   AUDITCON displays menu 1200. This is a read-only display that presents the audit status for your current container audit trail. You can open this display from various places in the container audit menu tree.

2. **Press the** Esc **key to return to the calling menu.**

Figure 5-8
Menu 1200: Audit Status

AUDIT STATUS	
Auditing status:	On
Audit file size:	2222
Audit file size threshold:	921600
Audit file maximum size:	1024000
Audit record count:	5

The "Audit status" menu displays the following status information for the current container audit trail:

Audit Status Information	Description
Auditing status	Shows as ON if auditing is enabled for the selected container audit trail, or OFF if auditing is not enabled.
Audit file size	Shows the size, in bytes, of the current container audit file.
Audit file size threshold	Shows the configured size at which the server sends warning messages to the server console and system log file.
Audit file maximum size	Defines the nominal maximum size for the audit file.
Audit record count	Defines the number of audit records in the current audit file.

This display does not define the complete status of a container audit trail. See "Configuring Auditing" in this chapter for more information on viewing and setting the audit configuration.

The audit status shown in this menu applies only to the replica of the container that was selected. The audit file size and audit record counts might be different in other replicas of the audit file.

Enabling Container Auditing

NetWare Enhanced Security is installed with auditing disabled for each container. Consequently, you must enable auditing to begin to accumulate container audit data.

The first time you enable auditing, AUDITCON creates an Audit File object for the container audit trail you're enabling. This Audit File object remains in place when you disable auditing.

To enable auditing for a container with a password, one of the two following conditions must exist:

(1) The server that contains the master replica must have the parameter "Allow Audit Passwords" set to ON.

or

(2) the server you are logged in to must have a replica of the partition that contains the container you want to audit.

Under the second condition, choose “Change Replica” from the “Available Audit Options” menu, then choose the server containing the read/write replica and set “Allow Audit Passwords” to ON for the server containing the replica.

When the auditor logs in to audit the container, the auditor will be prompted for a password for the container. This password is the one specified by the administrator. Once the auditor is logged in to the container, he or she must change the password to protect the data.

Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ You must have the Read right to the container object's Audit File Link property. This is necessary for AUDITCON to determine the existence of an Audit File object for the container.
- ❑ If an Audit File object does not already exist for the container, you must have the Write right to the container object's Audit File Link property to modify the container's Audit File Link to point to the Audit File object.
- ❑ If an Audit File object does not already exist for the container, you must have the Create object right to the container object.

Procedures

1. **From menu 1010, choose the desired container to be audited and press** F10**.**
2. **To enable auditing of the container, choose “Enable container auditing” from the “Available audit options” menu.**

   This option is available only in menu 1102 (when auditing is not already enabled for the container). AUDITCON then checks the container object’s Audit File Link to determine whether the container already has an Audit File object; if so, AUDITCON enables auditing and returns to menu 1101.

If the container does not have an Audit File object (for example, auditing was not previously enabled for this container), AUDITCON creates an Audit File object in the container.

The name of the Audit File object is "AFO*id_contname*," where *id* is a counter used if there is already an object with the desired name, and *contname* is the name of the container. For example, if the container name is FINANCE.ACME, then the Audit File object would be named AFO0_FINANCE.ACME, or if that object already exists, then AFO1_FINANCE.ACME.

If having an independent auditor is important to you, you might want to set the Access Control List and Inherited Rights Filter for the Audit File object to prevent access by administrators who are not auditors.

AUDITCON builds links from the Audit File object and Container object to each other. The server gives you the Supervisor object right to the Audit File object, and the Write right to the Object Trustees (ACL) property. In addition, AUDITCON gives you Read and Write rights to the Audit File object audit Policy property, and Read rights to the Audit Contents property. See "Controlling Access to Online Audit Data" on page 17 for information on giving other auditors rights to the Audit File object.

AUDITCON enables auditing for the container and returns to menu 1101.

When auditing is enabled for the first time on a container, there are no events selected. You should continue by using menu 1497, 1498, or 1499 (depicted on the following pages) to select the desired audit events.

When the server creates the audit file, it defines a password hash that can never be matched by a hashed password submitted by AUDITCON. If you intend to permit password-based access to the audit files, you must set the console parameter ALLOW AUDIT PASSWORDS=ON and use AUDITCON ("Auditing configuration" menu, "Change audit password" or "Set audit password" menu) to set an audit password for the audit files. (Do not configure the server to use audit passwords if you are using the server in a NetWare Enhanced Security configuration.)

See note under "Change Replica" in this chapter for additional information.

Configuring Auditing

This section describes how you can use AUDITCON's container audit configuration menu to define

- Which NDS events are audited
- How audit files are handled (size, threshold, rollover handling)
- How to set audit passwords
- How to disable auditing
- How to recover from audit file overflow

Auditing Configuration Prerequisites

- ❑ See "General Prerequisites" on page 29.
- ❑ To change the auditing configuration in a NetWare Enhanced Security configuration, you must have the Write right to the Audit Policy property of the Audit File object associated with the container you want to audit. If audit passwords are enabled at the server and you have logged in with the correct password, AUDITCON will also permit you to change the audit configuration.

  If the audit file is configured for level 2 passwords, and you don't have NDS access, then you must have the level 2 password to modify the auditing configuration. If you've logged in with a level 1 password, AUDITCON prompts for the level 2 password after each operation. These screens are not shown in the following sections because they don't pertain to the NetWare Enhanced Security configuration. See "Controlling Access to Online Audit Data" on page 17 for information on password levels.
- ❑ Determine what actions you want to perform (for example, which events to audit, how large you want the audit file to be) before you run AUDITCON.

Procedure

1. **Choose "Auditing Configuration" from the "Available audit options" menu (1101).**

AUDITCON displays menu 1497, 1498, or 1499, which list more configuration options, depending on the setting of the ALLOW AUDIT PASSWORDS option and whether you have sufficient rights to the Audit File object. See “Getting Started” on page 141 for the definition of sufficient rights.

Table 5-2 summarizes the algorithm AUDITCON uses to determine which menu it will display, based on the above two variables. Entries in italics will not occur in the NetWare Enhanced Security configurations.

Table 5-2
Container Audit Configuration Menu Selection

Allow Audit Passwords = ON	Sufficient Rights	Menu
Yes	*Yes*	*1497*
Yes	*No*	*1498*
No	Yes	1499
No	No	1499

Figure 5-9
Menu 1497: Auditing Configuration

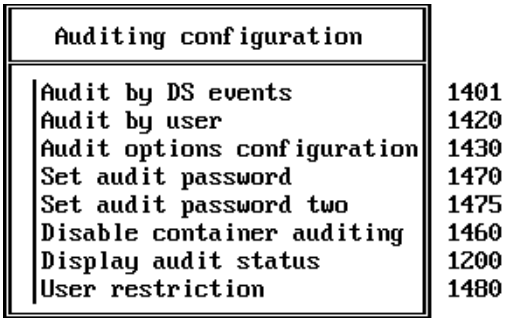


Figure 5-10
Menu 1498: Auditing Configuration

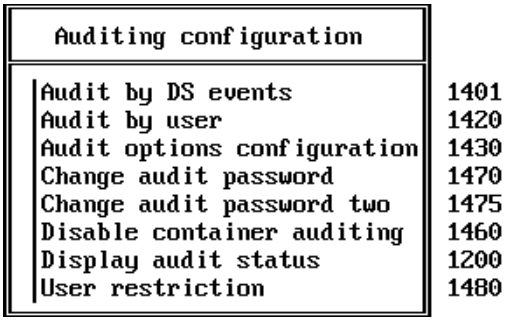
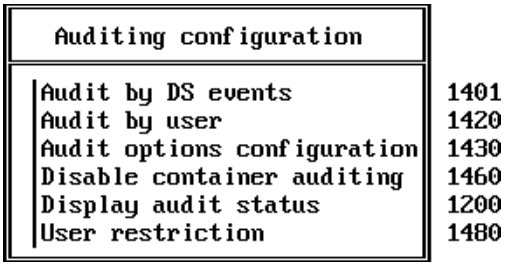


Figure 5-11
Menu 1499: Auditing Configuration



2. **Choose the desired configuration option, and press** Enter**.**

   These configuration submenus are addressed in the following sections.

Warning

When you make changes to the container audit configuration, you might receive a message that AUDITCON was unable to update the Audit File object. If this occurs, it is possible that your configuration changes could be lost.

Configuration of each container audit trail must be performed on a single server which holds a replica of the audit trail. It doesn't matter which one you pick, but all auditors of the container must use that one copy. Failure to use a single copy for configuration can cause unexpected results and/or loss of configuration changes.

Audit by DS Events

This section describes how you preselect the NDS events to be audited in the container audit file. Preselection is the operation of telling the server, in advance, which types of audit events you want the server to record in an audit file. By preselecting the events that are important in your organization, you conserve disk space for recording other audit events.

By default, the events you select will be recorded for all users of the container. If you only want to audit actions of certain users, you should set the “User restrictions” flag in the “User restriction” menu, and then preselect the specific users whose actions you want to record using the “Audit by user” menu.

You cannot generate audit reports for events or users that were not preselected for auditing when the event occurred. For example, if you need to review logins by a user two weeks ago, but you did not have logins preselected at that time, you will not be able to generate an audit report for these events. You must balance your need for certain audit information with the resources required to audit those events.

Prerequisites

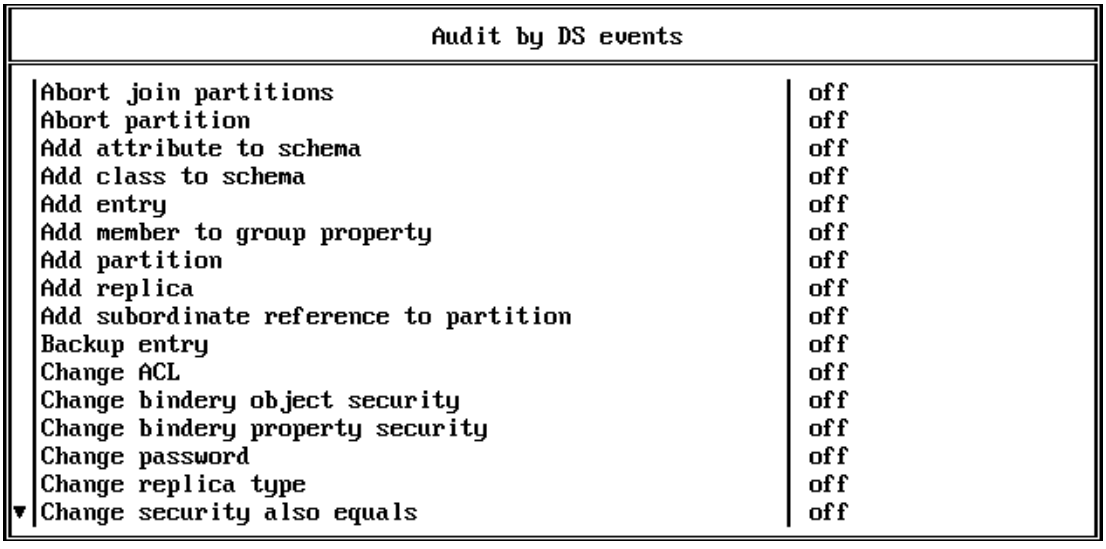
❑ See “General Prerequisites” on page 29 and the “Auditing Configuration Prerequisites” on page 155.

Procedures

1. Choose “Audit by DS events” from the “Auditing configuration” menu (1497, 1498, or 1499).

AUDITCON displays menu 1401 which lists the NDS events that you can preselect for auditing. These events are usually associated with user actions performed at client workstations, and the audit record includes the identity of the user that requested the service.

Figure 5-12
Menu 1401: Audit by DS Events



The following additional events can be displayed by scrolling the "Audit by DS events" screen.

Change security equivalence
Change station restriction
Clear NDS statistics
Close bindery
Compare attribute value
Create backlink
Create bindery property
Disable user account
Enable user account
End replica update
End schema update
Inspect entry
Intruder lockout change
Join partitions
List containable classes
List partitions
List subordinates

Log in user
Log out user
Merge entries
Merge trees
Modify class definition
Modify entry
Move entry
Mutate entry
Open bindery
Open stream
Read entry
Read references
Receive replica update
Reload NDS software
Remove attribute from schema
Remove backlink
Remove bindery property
Remove class from schema
Remove entry
Remove entry directory
Remove member from group property
Remove partition
Remove replica
Rename object
Rename tree
Repair time stamps
Resend entry
Send replica update
Send / receive NDS fragmented request / reply
Split partition
Start partition join
Start replica update
Start schema update
Synchronize partitions
Synchronize schema
Update replica
Update schema
User locked

Verify console operator

Verify password

In addition to the events that are preselected for auditing, container audit trails also include pseudo-events that establish the context for reviewing audit events. For example, the server records logins and logouts for users in other containers, even if logins and logouts are not selected for the current container.

2. **Determine the list of events that you want to audit. Move the cursor to each event and press** F10 **to toggle it to OFF or ON.**

   You can press F8 to toggle all events to ON or OFF.

3. **When you have set and reviewed the audit event configuration, press** Esc**.**

4. **Choose "Yes" to save the changes and return to menu 1497, 1498, or 1499, or "No" to leave the audit events unchanged.**

   If level 2 passwords are enabled, AUDITCON will prompt for the level 2 password before making the change.

Audit by User

By default, selected container events are recorded for all users. If you want to preselect by user for container events, then you must use the "User restriction" menu to set the "User restrictions" flag for the container to "Yes". The "User restriction" menu is reached from the "Auditing Configuration Menu."

If an auditor has rights to audit any volume or container in the network, that auditor is able to enable or disable auditing for any user in the Directory tree.

When you select a user for container auditing, the selection applies to all volumes and containers on all servers in the network. You cannot select user BOB for auditing of events on container LAB1.ENGR.ACME without also having BOB audited for events on all other volumes and all other containers in the network.

The server keeps user audit flags in the associated User objects in NDS, but does not save that information when you back up NDS. If you ever restore NDS from a backup, the audit flags will be lost. You must keep a manual record of all users you've preselected for auditing to restore that information.

Table 5-3 shows a sample form for recording which users have been marked for auditing. You must keep a record of all such users for recovery purposes. If NDS is ever restored from a full backup, you will use this list to reconstruct your audit settings. Failure to keep such a record and use it can result in loss of audit data.

Table 5-3
Sample Format for User Auditing Settings

Date	Time	Set/Cleared	NDS User Object Name
23 Mar 96	3:45pm	Set	CN=SALLY.O=ACME
23 Mar 96	3:48pm	Set	CN=HENRY.O=ACME
24 Mar 96	8:12am	Set	CN=FRED.OU=SALES.O=ACME
25 Mar 96	11:32am	Clear	CN=SALLY.O=ACME
25 Mar 96	11:50am	Set	CN=JULIE.OU=ENGR.O=ACME

Because NDS is a distributed system and some servers might be offline at any given time, selecting a user for auditing might involve a long delay before NDS can synchronize this information throughout the network. See Chapter 9, “Security Supplement to Maintaining the NetWare Server” of *NetWare Enhanced Security Administration* for information on how to determine that a change has been synchronized to all replicas of the partition on which it resides.

Prerequisites

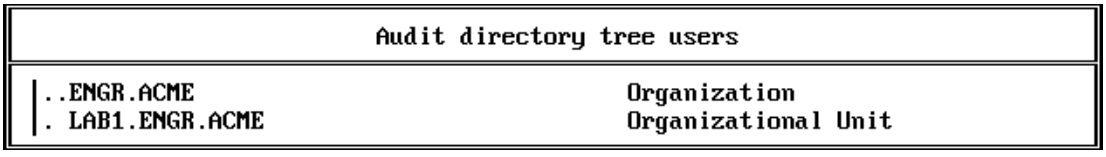
- ❑ See“General Prerequisites” on page 29 and “Auditing Configuration Prerequisites” on page 155.
- ❑ You do not need specific rights to a User object in the NDS database to set the audit flag for that user.

Procedures

1. **Choose “Audit by user” from the “Auditing configuration” menu (1497, 1498, or 1499).**

   AUDITCON displays menu 1420, which lists containers that can hold User objects.

Figure 5-13
Menu 1420: Audit Directory Tree Users



2. **Choose the container that holds the User objects and press** Enter**.**

   AUDITCON expands the menu to list the objects in that container.

3. **To preselect a user for volume and container auditing, use the up and down arrow keys to scroll within the window. Choose a user and press** F10 **to toggle the user audit flag to ON or OFF.**

   You can preselect users in other containers by selecting the container, which will then show the users in that container. Non-User objects (for example, Organizational Unit objects) are displayed, but you cannot toggle the audit flag for those objects.

4. **When you have set and reviewed the audit event configuration, press** Esc**.**

5. **Choose "Yes" to save the changes and return to menu 1420, or choose "No" to leave the audit events unchanged.**

Note Setting the audit flag on the USER_TEMPLATE user will not cause automatic auditing of newly created users. When a new user is created, you must preselect his or her NDS User object if you want the user's actions to be audited.

Audit Options Configuration

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29 and “Auditing Configuration Prerequisites” on page 155.

Procedures

Procedure

1. Choose “Audit options configuration” from the “Auditing configuration” menu (1497, 1498, or 1499).

AUDITCON displays menu 1430, which defines the current audit configuration for the container audit trail.

Figure 5-14
Menu 1430: Audit Configuration

```
                    Audit configuration

Audit file maximum size:                                1024000
Audit file threshold size:                               921600
Audit overflow file size:                                102400
Automatic audit file archiving:                              No
Days between audit archives (1-255):
Hour of day to archive (0-23):
Number of old audit files to keep (1-15):                    15
Allow concurrent auditor logins:                             No
Broadcast errors to all users:                               No
Force dual-level audit passwords:                            No
 Error recovery options for audit file full
Archive audit file:                                          No
Disable auditable events:                                   Yes
Disable event recording:                                     No
Minutes between warning messages:                             3
```

The following list describes the available configuration parameters for container auditing. The first ten parameters (“Audit file maximum size” through “Force dual-level audit passwords”) are the same for container auditing and volume auditing. For more information on these parameters, refer to the description of the corresponding volume configuration parameters in “Audit Options Configuration” in Chapter 4 of this manual.

The line “Force dual-level audit passwords” is omitted if the ALLOW AUDIT PASSWORDS console parameter is OFF, as required in the NetWare Enhanced Security configuration.

When computing the overflow audit file size for a container audit trail, you must use the maximum value for the number of service processes on all servers where the container is stored. That is, if the container is stored on servers A, B, and C, you must use the highest value for the number of service processes in your calculation. Otherwise, your value might not be large enough and you could lose some audit data.

The server provides three options for handling container audit file overflow. The options, as shown in Table 5-4, " Overflow Options", are "Archive audit file," "Disable audited events," and "Disable event recording."

Table 5-4
Overflow Options

Archive audit file	With this setting, the server archives the current audit file and creates a new audit file. If necessary (because the maximum number of old online audit files already exists), the server deletes the oldest of the old online audit files. This option is not recommended for use in NetWare Enhanced Security networks because it can result in audit data being lost.
Disable audited events	With this setting, the server disables all audited NDS events when the current audit file has reached the "Audit file maximum size" or the server cannot write to the current audit file (for example, it is out of disk space). The server doesn't attempt to roll over to a new audit file, even if audit files and disk space are available. In this overflow state, any event that is preselected for auditing is disabled; however, events that are not preselected are still permitted. For example, if logins are preselected for auditing, any attempt to log in to an object in the container (except by an auditor) will fail. This is the only overflow option that guarantees that you will not lose audit data. Consequently, if collection of audit data is of the utmost importance (such as, in a NetWare Enhanced Security network), then you should use this setting, even though it might inconvenience users when they are unable to log in to perform other NDS actions.

Table 5-4 *continued*
Overflow Options

Disable event recording	With this setting, the server turns off auditing and stops entering new audit records into the current audit file when it reaches the maximum size limit or when an unrecoverable write error occurs for the audit file. The server doesn't attempt to roll over to a new audit file, even if there is disk space for archiving the current audit file. You must reset the current audit file to re-enable event recording. Until you re-enable event recording, users can access the NDS container without any audit coverage. Consequently, this setting is not recommended for use in NetWare Enhanced Security networks because it can result in audit data not being recorded.
Minutes between warning messages	The server sends warnings to the console at this frequency if the audit file is full and the overflow option is configured to either "Disable audited events" or "Disable event recording". If you have the "Archive audit file" option configured, then a warning message is sent when the audit file is almost full, but there is no additional message when the archive occurs.

2. **Move the cursor to the field you want to change and enter the new configuration value.**

   For numeric fields (for example, "Audit file maximum size"), type the new value into the field over the previous value, then press Enter. For "Yes / No" settings, type "Y" or "N" to change the value. Depending upon your change, the server might modify other values on the configuration screen. For example, if you set "Automatic audit file archiving" to "No", the server will blank out the entries for "Days between audit archives" and "Hour of day to archive."

   If you enable "Force dual-level audit passwords," AUDITCON will immediately prompt you (twice) to enter the new level 2 password. These menus are not shown here, because audit passwords are not permitted in NetWare Enhanced Security networks.

3. **Review the settings on the current screen, and change any settings as needed.**

4. **When you are finished, press** Esc **to exit the menu.**

5. **Choose "Yes" to save the changes and return to menu 1497, 1498, or 1499, or choose "No" to leave the audit configuration unchanged.**

Audit files consume disk resources that might be needed by other users. Before you define the number and size of audit files, discuss your projected disk space requirements with an administrator for each server that holds a replica of the container.

The server's NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. Do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON) because this violates the assumptions under which the server was evaluated.

Change Audit Passwords

"Controlling Access to Online Audit Data" on page 17 describes the use of the password-based mechanism for accessing audit files. This section describes how to change both level 1 and level 2 passwords. This section is applicable only if the ALLOW AUDIT PASSWORDS option is set to ON.

This procedure assumes that the auditor (not the system administrator) is the one performing these procedures and that the administrator has previously established the passwords and has shared them with the auditor. The auditor can change the level 1 password after logging in to the container.

The server's NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. For NetWare Enhanced Security networks, do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console) because this violates the assumptions under which the server was evaluated.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Auditing Configuration Prerequisites" on page 155.

Procedures

1. **To change the level 1 password, choose "Change audit password" from the "Auditing configuration" menu (1497, 1498, or 1499).**

Enter the current (level 1) audit password as prompted by AUDITCON.

AUDITCON does not echo any password information to the screen.

If dual-level passwords are enabled, AUDITCON prompts you to enter the level 2 password before you can change the level 1 password. AUDITCON allows you to change the level 2 password using the same procedure used to change the level 1 password.

2. **Enter the new (level 1) audit password when prompted by AUDITCON.**

   AUDITCON prompts you twice for the new password. This ensures that the auditor did not make an error when entering the password.

   AUDITCON does not check the password for length, alphanumeric characters, or other characteristics of strong passwords, nor does it ensure that it is different from the previous password. Uppercase and lowercase characters are treated identically.

If you use audit passwords to control access to the audit file, be sure not to reuse your server password as the audit password.

Set Audit Passwords

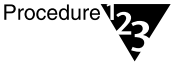
"Controlling Access to Online Audit Data" on page 17 describes the use of the password-based mechanism for accessing audit files. This section describes how to set level 1 passwords and level 2 passwords (if level two passwords are enabled).

The server's NetWare Enhanced Security configuration requires use of the NDS rights-based access control mechanism to protect audit data. For NetWare Enhanced Security networks, do not enable the password-based access control method (by setting ALLOW AUDIT PASSWORDS=ON at the server console) because this violates the assumptions under which the server was evaluated for C2 status.

Prerequisites

❑ See "General Prerequisites" on page 29 and "Auditing Configuration Prerequisites" on page 155.

Procedures



1. **To set the level 1 password, choose "Set audit password" from the "Auditing configuration" menu (1497, 1498, or 1499).**

   AUDITCON prompts you to enter the new (level 1) container password.

2. **Enter the new password as prompted by AUDITCON.**

   AUDITCON does not echo any password information to the screen

   If dual-level passwords are enabled, AUDITCON prompts you to set the level 2 password before you can set the level 1 password. AUDITCON allows you to set the level 2 password using the same procedure used to change the level 1 password.

   AUDITCON then prompts you to reenter the new password.

3. **Reenter the new password when prompted by AUDITCON.**

   This ensures that the auditor did not make an error when entering the new password.

   AUDITCON does not check the password for length, alphanumeric characters, or other characteristics of strong passwords, nor does it ensure that it is different from the previous password. Uppercase and lowercase characters are treated identically.

   If dual-level passwords are enabled, AUDITCON prompts for you to enter the level 2 password before it will change the level 1 password.

If you use audit passwords to control access to the audit file, be sure not to reuse your server password as the audit password.

If you use a password to control access to an audit file, and forget the audit password, then you must use the rights-based as described in "Controlling Access to Online Audit Data" on page 17. Once you have access to the audit trail, you can reset the password as described in this section.

Disabling Container Auditing

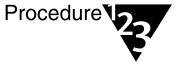
When you disable container auditing, you stop the server from recording audit events to the container audit file, but you do not delete the Audit File object for the container audit trail. The Audit File object remains, and is reused (to provide an initial configuration) if you re-enable auditing for the container.

After container auditing has been disabled, it can be re-enabled using the Enable External Auditing menu (see "Enabling Container Auditing" on page 152).

Prerequisites

❑ See "General Prerequisites" on page 29 and "Auditing Configuration Prerequisites" on page 155.

Procedure



1. **Choose "Disable container auditing" from the "Auditing configuration" menu (1497, 1498, or 1499).**

2. **Choose "Yes" and press** Enter **to disable auditing, or choose "No" to continue auditing.**

   AUDITCON returns to menu 1010.

User Restriction

This menu provides for setting the following audit control flags in the current container's Audit File object Audit Policy.

- **User Restriction**. By default, when you preselect a container event (see "Audit by DS Events"), the events you select are audited for all users. However, if you set the "User restriction" flag, the server audits only those users that have been specifically preselected for auditing (see "Audit by User").

- **Audit NOT_LOGGED_IN**. Before a user logs in to NDS, the server permits the user to perform limited searches through the Directory (see the NDS chapters in *NetWare Enhanced Security Administration*). By default, the server does not audit these unauthenticated user events. However, if you set the "Audit

NOT_LOGGED_IN users" flag, the server will record these events in the current container audit file.

These flags pertain only to the currently selected container and do not affect other container or volume audit files. Unlike the per-user audit flag (which is global across the network), the "User restriction" and "Audit NOT_LOGGED_IN users" flags must be set individually for each volume and container. The two flags are independent of each other, so you can set either flag without affecting the other.

Warning

If you set the "User restrictions" flag to "Yes", you must also preselect those users you want audited, using the procedures shown in "Audit by User" in Chapter 4 or "Audit by User" on page 161 in Chapter 5. Setting the "User restrictions" flag to "Yes" without preselecting any users will mean that no container events will be recorded in the audit trail.

If you set the "User restrictions" flag to "Yes" but leave the "Audit NOT_LOGGED_IN users" flag set as "No", then actions of unauthenticated users will not be audited.

Unlike the per-user audit flag (which is global across the network), the "User restrictions" and "Audit NOT_LOGGED_IN users" flags must be set individually for each volume and container and apply only to that volume or container.

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Auditing Configuration Prerequisites" on page 155.

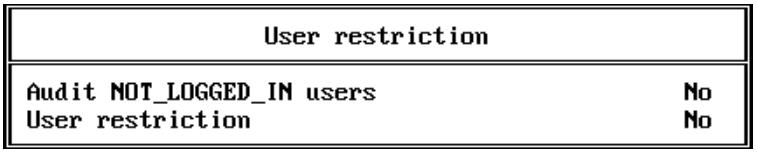
Procedures

Procedure

1. Choose "User restriction" from the "Auditing configuration" menu (1497, 1498, or 1499).

AUDITCON displays menu 1480, which allows you to select the user restriction parameters for the container.

Figure 5-15
Menu 1480: User Restriction



2. Review the settings on the current screen, and change any settings as required.

Press “Y” to set a value to “Yes” or press “N” to set the value to “No”.

3. **When you are finished, press** Esc **to exit the menu.**

4. **Choose “Yes” to save the changes and return to menu 1497, 1498, or 1499, or choose “No” to leave the user restrictions configuration unchanged.**

Generating Container Audit Reports

AUDITCON allows you to process online and offline audit files to extract and review the information the server has collected for you. Processing consists of displaying audit information on the AUDITCON screen (viewing) and generating printable reports (printing).

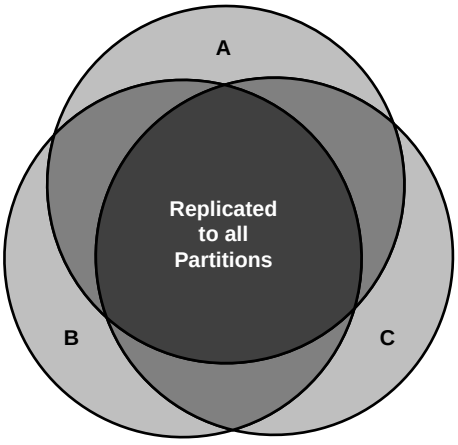
This section describes how to process online audit files, that is, either the current audit file or old audit files that have been archived (that is, rolled over) by the server but are still maintained as audit files by the server. See “Generating Reports from Offline Audit Files” on page 204 for information on how to process offline audit files.

One significant difference between volume and container auditing is that container audit records are replicated to each server that contains a replica of the audited container. That is, if container SALES is replicated on three servers (A, B, and C), then users can access an object in the container, for example, BART.SALES, on any of the three servers. If a user accesses the replica of BART.SALES on server C, then server C generates an audit record in its local audit file and attempts to replicate the audit record to the audit files on servers A and B.

The container audit files exist on the servers where the container is replicated. These might or might not be the same servers where the container Audit File object is replicated.

The replication of audit records is similar to, but is not as reliable as, the replication of NDS objects. DS.NLM provides a high degree of confidence that changes to an NDS object (for example, BART.SALES) are replicated to all partitions holding the object. However, there are circumstances where audit records might not be replicated by one server to another.

The following figure shows that each of the three servers (A, B, and C) record a high percentage (for example, 99%) of all of the audit records, however, each of the servers might have audit records that were not successfully replicated to the other two servers.



In particular, any data that isn't replicated when a server archives (rolls over) a container audit file will never be replicated. For example, assume server C audits the access attempt to BART.SALES to its local SALES audit file, attempts to replicate the audit event to servers A and B, and then, subsequently, rolls over the audit file. If servers A and B are offline, disconnected, or do not have sufficient disk space when server C tries to replicate the audit record, then the audit record will not be copied to the audit files on those servers.

Warning

Because all container audit events are not necessarily replicated to all servers, some records might be missing from each copy. You must look at all of the audit trails to see the full history for the container. Thus, you should examine the audit trail on server A, then select a different replica (menu 1150) and review the audit trail for the container on server B, and repeat the process for server C.

Audit Report Prerequisites

Checklist

- ❏ See "General Prerequisites" on page 29.
- ❏ To process online audit files, you must either have the Read right to the Audit File object Audit Contents property or have logged in to the audit trail. (To log in to an audit trail, you must enable audit passwords at the server console. This configuration is not permitted in NetWare Enhanced Security facilities.)

- ❑ You must have the ability to create new (temporary) files in the directory you were in when you started AUDITCON, and sufficient disk space on that volume. These temporary files are used to hold the audit data as it is extracted from the audit trail.

- ❑ Remember that you can only view or report audit events that have been recorded by the server. For example, if you do not configure the server to record Change ACL events, then you cannot display any Change ACL events. Consequently, to generate meaningful audit reports, you must first preselect those events for auditing. (See "Audit Options Configuration" in this chapter for more information on preselecting container audit events.)

Warning

Because AUDITCON places temporary files in the directory you were in when you started AUDITCON, and these temporary files contain audit data, you must not generate any reports unless your current directory is protected from access by users who are not authorized to see audit data.

Procedures

Procedure

1. **Choose "Auditing reports" from the "Available audit options" menu (1101).**

   AUDITCON displays menu 1500.

Figure 5-16
Menu 1500: Auditing Reports

```
Auditing reports

Display audit status                1200
Edit report filters                 1501
Report audit file                   1525
Report audit history                1530
Report old audit file               1540
Report old audit history            1550
View audit file                     1560
View audit history                  1570
View old audit file                 1580
View old audit history              1590
Database report audit file          1800
Database report audit history       1810
Database report old audit file      1820
Database report old audit history   1830
```

2. **Choose the desired auditing report option, and press** Enter**.**

   You have several options available for creating and viewing reports from the records in audit files.

- You can create filters to extract specific information (for example, events or times) from the audit file, or you can view all the records in an audit file. Unless you are just browsing the audit trail, you would normally want to define one or more report filters before you generate an audit report or view an audit file.

- Process the current audit file (for example, “Report audit file”) or process an old audit file (for example, “Report old audit file). References to old audit files explicitly indicate operations on one of the server’s old audit files, while the other operations are implicitly on the current audit file.

- You can direct output to your AUDITCON screen (for example, “View audit file”) or send the output to a file on your workstation or a directory on the server (for example, “Report audit file”).

- You can extract information about client user events (for example, “View audit file”) or extract information about auditor events (for example, “View audit history”). The audit file contains user events, while the audit history file contains a record of actions by the auditor in managing the audit trail.

  The audit history is actually included in the audit file, and is not a separate file. It is described as the audit history file for compatibility reasons.

- You can cause reports to be generated as text (for example, “Report audit file”) or in a form suitable for loading into a database (for example, “Database report audit file”).

These options are addressed in the following sections.

Edit Report Filters

Note

The procedures described in this section allow you to generate filter files and report files on your local workstation. See your client documentation for details on how to use your workstation's security mechanisms to protect these files.

AUDITCON lets you create filters so you can extract the specific information that you want from an audit file. If you view a report without applying a filter, AUDITCON displays the entire contents of the file.

You can create as many filters as you want to screen information in the audit file. Then, any time you want to generate a report, you can select and apply the filter.

Warning

An audit filter is a DOS file that contains the filter information. By default, AUDITCON saves the filter file in your current working directory, which can be on a local drive on your workstation or on a network drive. The name of the file is typically the filter name, with a file extension of ".ARF" (for Audit Report Filter). While this allows you to create audit filters in a variety of different directories, AUDITCON does not provide a means for you to access filters in a different directory. Consequently, if you want to use a filter that you have previously defined, you must run AUDITCON from the directory where the filter is located, or copy the filter to your current directory before you run AUDITCON. Audit report filters must be protected from modification by storing them only in locations where they will be protected by NetWare or by client workstation access controls.

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and "Audit Report Prerequisites" on page 173.

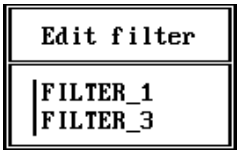
Procedure

Procedure

1. **Choose "Edit report filters" from the "Auditing reports" menu (1500).**

   AUDITCON displays menu 1501, which lists the filters you have previously defined. If you have not defined any filters in the current directory, AUDITCON displays a null entry "_no_filter_".

Figure 5-17
Menu 1501: Edit Filter

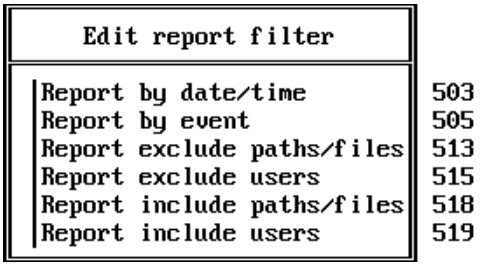


2. **At menu 1501, you can highlight an entry and press either** F10 **or** Enter **to select that filter for editing. Alternately, press** Insert **to create a new audit filter.**

   AUDITCON displays menu 1502, which shows the available filter criteria. The steps for creating a new filter and editing an existing filter are essentially the same.

   The primary difference is that if no audit filters exist, you can press Enter to create a new audit filter, but you cannot press F10 to edit.

Figure 5-18
Menu 1502: Edit Report Filter



3. **Choose the option (the criteria for printing an audit record) and press** Enter **to define the filter rules.**

   These include:

   - **Report by date/time.** Allows you to specify one or more time periods to include in a report. All audit records that match one of the time periods are candidates for reporting. If the date/time filter is empty (that is, no times are specified), all audit records are candidates for reporting.

   - **Report by event.** This filter allows you to specify the types of audited events to include in a report. All audit events that match the specified events are a candidate for reporting. For example, if you specify create directory and file open events in a filter, your report will include only create directory and file open events.

   - **Report exclude users.** This filter allows you specify one or more users that you want to exclude from audit reports. All other users are potentially included.

   - **Report include users.** This filter allows you to specify one or more users that you want to be included in the report. The

default is an asterisk (*), which indicates that all users can be reported.

When you create an audit report, AUDITCON applies these filters to records that it reads from the audit file. AUDITCON reports only those events that match all the filter criteria. That is, the audit record time stamp must match the date/time filter and the audit record event type must match the event type filter, and so on. If a filter contains conflicts between "include" and "exclude" options, the "exclude" option takes priority.

Report by Date/Time

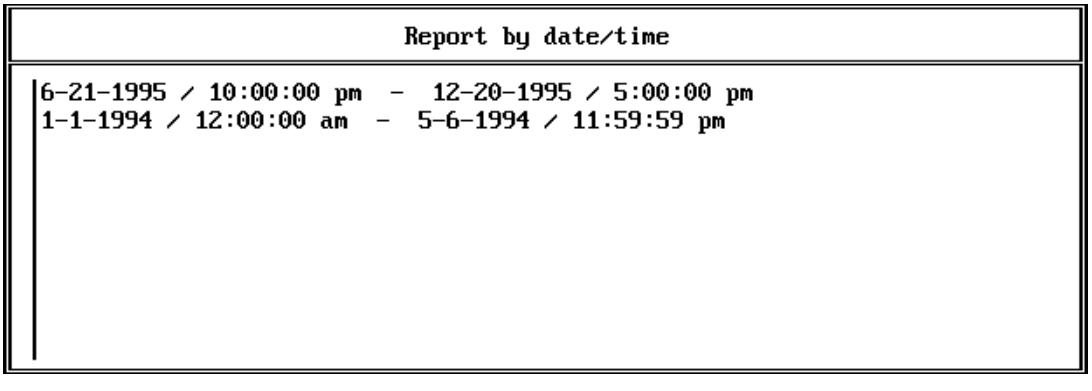
Procedure

Procedure

1. **Choose "Report by date/time" from the "Edit report filter" menu.**

   AUDITCON displays menu 1503, which lists the existing date/time ranges defined for the filter. If you are inserting a new filter, this menu will initially be empty.

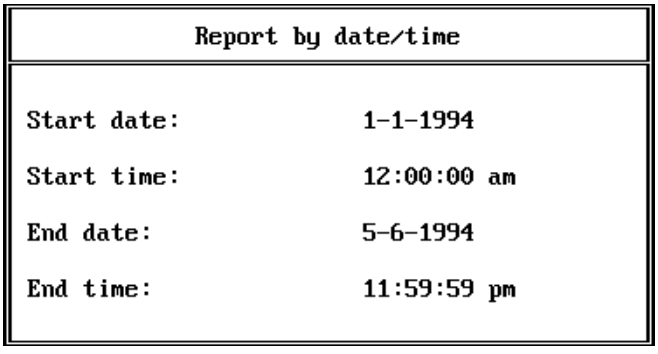
Figure 5-19
Menu 1503: Report by Date/Time



2. **Highlight an entry and press** Enter **to edit an existing date/time range, or press** Insert **to define a new range, or highlight an entry and press** Delete **to remove a time range from the filter.**

If you press Insert or Enter, AUDITCON displays menu 1504, which allows you to do more editing of the date/time profile selected in menu 1503.

Figure 5-20
Menu 1504: Report by Date/Time



3. To edit the date/time profile, use the arrow keys to move the cursor to the desired field and type in the new value.

AUDITCON makes reasonable attempts to convert alternate forms (for example, "3/15/95", "mar 15", "15 Mar 95", "8am", or "8a") into the standard format.

4. When you are finished and have reviewed the date/time range, press Esc **to return to menu 1503.**

If AUDITCON finds an error (for example, the start date/time is later than the end date/time), it displays an error message and goes back to menu 1504.

Report by Event

Procedure

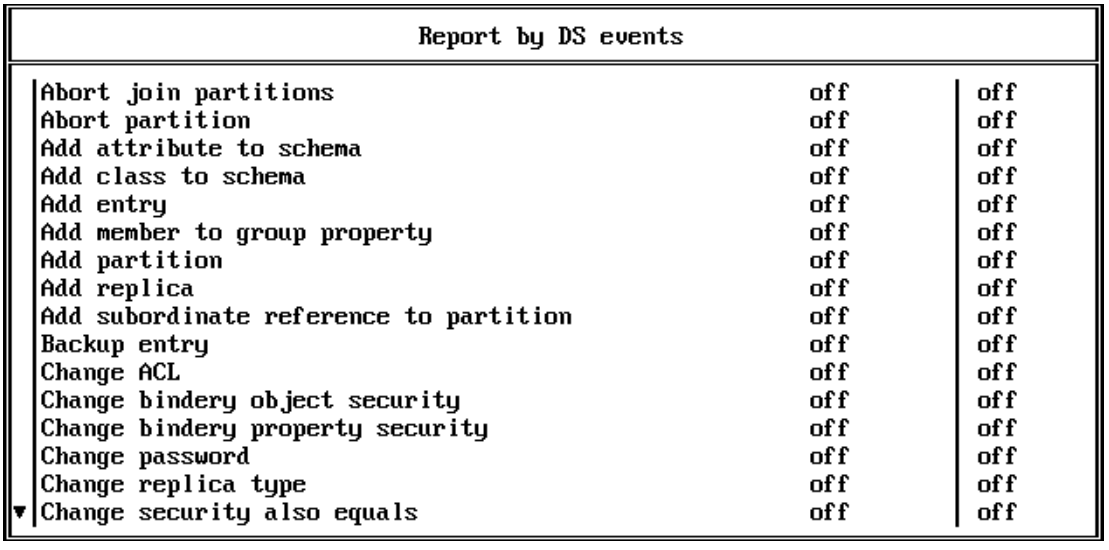
Procedure

1. Choose "Report by event" from the "Edit report filter" menu.

AUDITCON displays menu 1505, which provides a high-level selection of the types of DS audit events defined in the current filter. This menu has three columns: a DS event type (left column); an indication of whether the event is preselected for auditing in the current audit file (middle column); and flags for toggling the event ON or OFF in the current audit filter (right column).

The preselection indication is with respect to the current audit file, and might bear no significance to the events that are actually recorded in the audit files to which the filter is applied.

Figure 5-21
Menu 1401: Report by DS Events



The following additional events can be displayed by scrolling the Audit by DS events screen.

Change security equivalence
Change station restriction
Clear NDS statistics
Compare attribute value
Create backlink
Create bindery property
Disable user account
Enable user account
End replica update
End schema update
Inspect entry
Intruder lockout change
Join partitions
List containable classes

List partitions
List subordinates
Log in user
Log out user
Merge entries
Merge trees
Modify class definition
Modify entry
Move entry
Mutate entry
Open stream
Read entry
Read references
Receive replica update
Reload NDS software
Remove attribute from schema
Remove backlink
Remove bindery property
Remove class from schema
Remove entry
Remove entry directory
Remove member from group property
Remove partition
Remove replica
Rename object
Rename tree
Repair time stamps
Resend entry
Send replica update
Send/receive NDS fragmented request/reply
Split partition
Start partition join
Start replica update
Start schema update
Synchronize partitions
Synchronize schema
Update replica
Update schema

User locked
Verify console operator
Verify password

2. **To change the DS events in the current filter, choose the event and press** F10 **to toggle the setting for that event in the right column. When you are finished, press** Esc **to return to menu 1502.**

Report Exclude Users

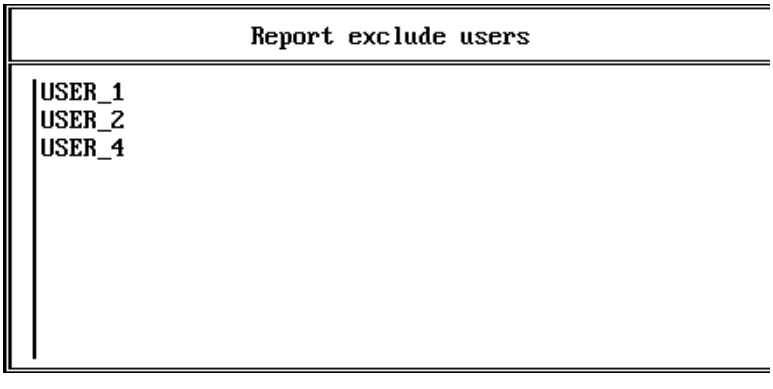
Procedure

Procedure

1. **Choose "Report exclude users" from the "Edit report filter" menu.**

   AUDITCON displays menu 1512, which lists the audit filter's users to be excluded from audit reports.

Figure 5-22
Menu 1515: Report Exclude Users



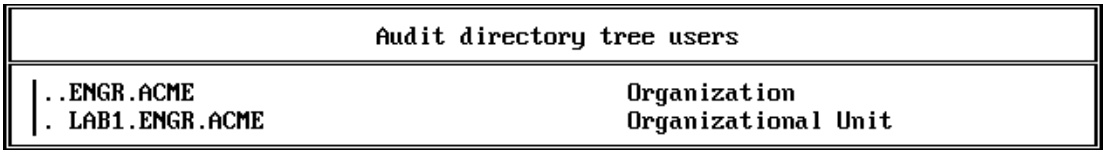
2. **Press** Enter **to enter a new user name or press** Delete **to remove an existing entry.**

   To return to menu 1502, press Esc.

3. **If you pressed either** Enter **or** Delete **you can enter or edit a user name. Press** Enter **to add the user name to the exclude list.**

   If you want help with the list of users, press Insert and AUDITCON will display menu 1514 which shows containers that can hold User objects.

Figure 5-23
Menu 1514: Audit Directory Tree Users



4. **Choose the container that holds the User object and press** Enter**.**

   AUDITCON expands the menu to list the objects in the container.

Note

AUDITCON does not verify that the usernames entered are valid. If they are not valid, they are simply ignored.

5. **Choose the user you want to include or exclude from the audit report and press** Enter **to add the name to the list.**

   If the user's name does not appear in this list, return to menu 1514 and browse the Directory tree by listing other containers until the user's name appears.

Report Include Users

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" in this chapter.

Procedure

Procedure

1. **Choose "Report include users" from the "Edit report filter" menu.**

   AUDITCON displays a list of the audit filter's users to be included in audit reports. Initially, this menu contains only an asterisk to indicate that all users are included, but you can edit the menu (as described for "Report exclude users") to specify a few users.

2. **When you have finished defining all the filter criteria, return to the "Edit report filter" menu (1502) and press** Esc**.**

AUDITCON gives you the option of choosing “Yes” to save the changes or “No” to leave the filters unchanged.

If you choose “Yes” to save the changes, AUDITCON prompts you to enter the name of the filter file.

3. **Enter a filename for the filter you want to save.**

   The filter name can be up to eight characters long and must not contain a period.

   AUDITCON appends a “.ARF” extension to the filter name (for example, “FILTER_3.ARF”), and writes the filter file in the auditor's current directory.

Deleting an Audit Filter

Prerequisites

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” in this chapter.

Procedure

1. **To delete a selected audit filter, press** Delete **at menu 1501.**

   You can choose “Yes” to delete the .ARF file that contains the specified audit filter or choose “No” to leave the filter in place.

2. **Choose “Yes” to delete the filter.**

   AUDITCON displays menu 1501 and lists the remaining filters (.ARF files) in the current directory. If you have deleted the last remaining audit filter in the current directory, AUDITCON shows “_no_filter_” in menu 1501.

Report Audit File

This section describes how to generate a formatted text version of the user events in the current audit file. You cannot directly print the server’s audit files, because the server’s audit files are not directly accessible to network clients and the server’s audit files are stored in a compressed format.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

Procedure

1. **Choose “Report audit file” from the “Auditing reports” menu (1500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON tries to create the file and displays an error screen if it cannot.

Note

If you don’t specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 1521 to display the available filters. These include the files with .ARF extensions in your current directory and a null filter (“_no_filter_”) that will pass all records in the audit file.

Figure 5-24
Menu 1521: Select Filter

3. **To use one of the available filters, choose that filter and press** Enter**.**

AUDITCON also allows you to create a temporary filter, or modify an existing filter, for use in this report. Choose the desired filter (or "_no_filter_") and press F10. Edit the filter as described in "Generating Container Audit Reports" on page 172, then press Esc.

You are given the options of discarding the changes, saving the changes to a filter file, or applying the filter to the current report without saving the changes.

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.

Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process.

AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait" notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

4. **To review the contents of your report, exit to DOS and either print or use an editor.**

Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file.

Prerequisites

- ❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

1. **Choose “Report audit history:” from the “Auditing reports” menu (1500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

If you don’t specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a “Reading file” message in the header area of your screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

3. **To review the contents of your report, exit to DOS and either print or use an editor.**

Report Old Audit File

This section describes how to generate a formatted text version of the user events in an old online audit file.

Prerequisites

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

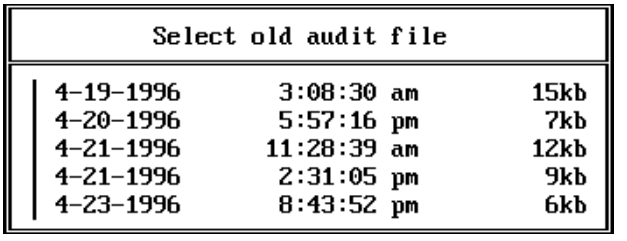
Procedures

Procedure

1. **Choose "Report old audit file" from the "Auditing reports" menu (1500).**

   AUDITCON displays menu 1540, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-25
Menu 1540: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the output file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 1542 to display the available filters.

Figure 5-26
Menu 1542: Select Filter

4. **Choose the desired filter and press** Enter**, or press** F10 **to edit a filter.**

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file. Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait" notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

5. **To review the contents of your report, exit to DOS and either print or use an editor.**

Report Old Audit History

This section describes how to generate a formatted text version of the auditor events in an old online audit file.

Prerequisites

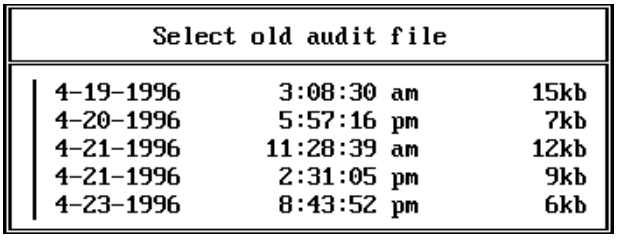
- ❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

1. **Choose "Report old audit history" from the "Auditing reports" menu (1500).**

   AUDITCON displays menu 1550, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-27
Menu 1550: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the output file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

4. **To review the contents of your report, exit to DOS and either print or use an editor.**

View Audit File

This section describes how to display a listing of the user events in the current audit file on the screen of your workstation.

Prerequisites

Checklist

- ❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" on page 172.

Procedures

Procedure

1. Choose "View audit file" from the "Auditing reports" menu (1500).

AUDITCON displays menu 1560 to display the available filters. These include the files with .ARF extensions in your current directory and a null filter ("_no_filter_") that will pass all records in the audit file.

If AUDITCON does not display the desired filter, return to DOS, change to the directory where the filter is located, and try again.

Figure 5-28
Menu 1560: Select Filter

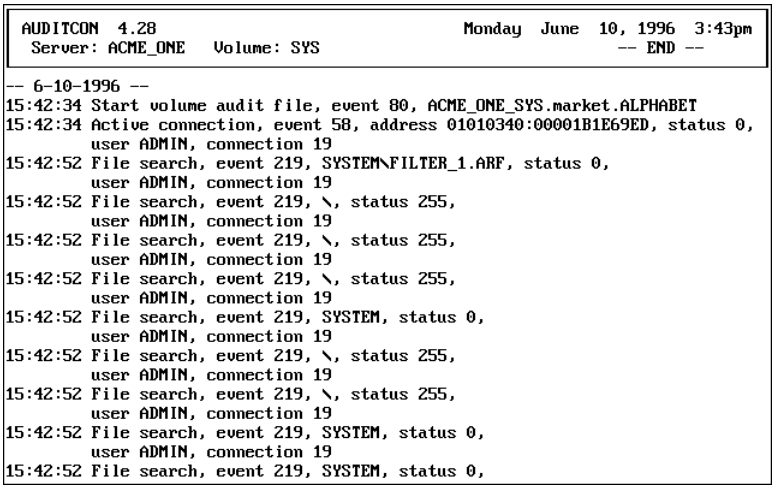
2. Choose the desired filter and press Enter**, or press** F10 **to edit a filter.**

If you choose a filter and press Enter, AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and displays the formatted records to your screen a page at a time.

The second line of the header area is modified to show your location in the audit file and when AUDITCON is waiting for information from the server. "-- HOME --" indicates the beginning of the file and "-- END --" indicates the end of the audit file.

At any time you can press Home to return to the beginning of the file, or End to go to the end of the file. Press Page Down or Page Up to display a new page of formatted audit records, or use the down- or up-arrow keys to change the display one record at a time.

Figure 5-29
Sample audit file



When AUDITCON is waiting for data from the server, it displays a “-- Reading file --” notification; otherwise, it displays “-- PAUSE --”.

AUDITCON displays the time (for example, “17:38:28”) for each audit record, but only displays the date (“-- 3-14-1995 --”) at the beginning of an audit file or when the date rolls over from one day to the next. The first record defines the start time of the audit file and the container context being audited.

Subsequent events define the name of the event (for example, “Change ACL”), a numeric event number (“107”), the change ACL arguments (“object grp1, add trustee [Root], attribute Member, rights [R]”), the status for the event (in this case, 0 indicates success), the name of the user making the change, and the replica where the audit event is being audited. Remember that if the audited container is replicated, the audit event can be synchronized to other replicas. See Appendix A, “Audit File Formats,” on page 267 for more information on the format of individual events.

If an audit event was generated as a result of an action by a user who was not logged in (typically, by a user looking for their NDS object using the CX or LOGIN utilities), then the user name will be _NOT_LOGGED_IN in place of the actual username.

If you have preselected login events, then you might see pairs of events for the same user, where the first entry in the pair indicates a failure, and the second indicates a success. This occurs because the LOGIN program first tries to log a user in without a password (thus generating an audit record for the failed attempt), and if that fails it prompts the user for a password, and uses that password for a second attempt. Thus, a failed login followed by a successful login probably does not indicate that the user has incorrectly typed his or her password.

3. **Press** Esc **when you are finished. AUDITCON requests confirmation that you are done. Choose "Yes" and press** Enter **to return to menu 1500.**

View Audit History

This section describes how to display a listing of the auditor events on the screen of your workstation.

Prerequisites

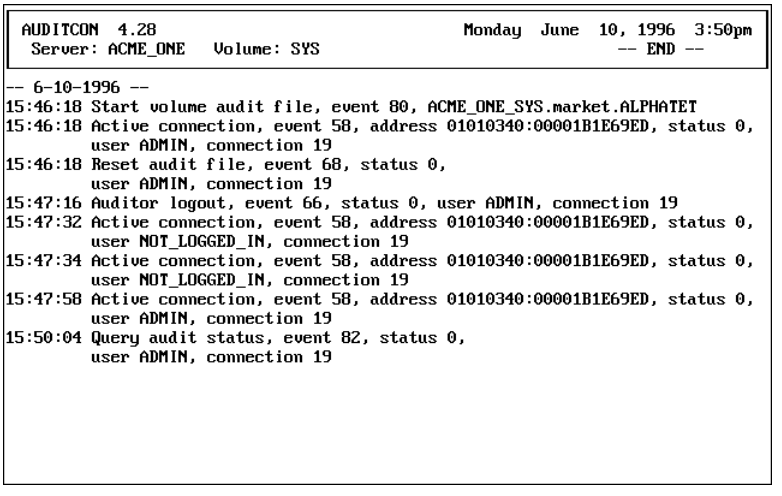
❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" on page 172.

Procedures

1. **Choose "View audit history" from the "Auditing reports" menu (1500).**

   AUDITCON reads the current audit file and displays the first screen of audit history events.

Figure 5-30
Sample audit history



2. **Use the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer "Yes" to return to menu 1500.**

Note

The "Auditor login" event means that an auditor began accessing the audit file, while the "Auditor logout" event means that an auditor ceased accessing the access file. These events do not indicate user logins or logouts.

View Old Audit File

This section describes how to display a listing of the user events from an old online audit file to the screen of your workstation.

Prerequisites

Checklist

❑ See "General Prerequisites" on page 29 and the Audit Report Prerequisites in "Generating Container Audit Reports" on page 172.

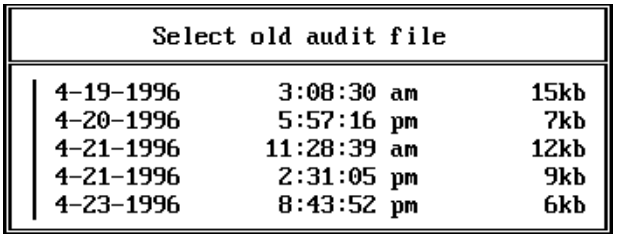
Procedures

Procedure

1. **Choose "View old audit file" from the "Auditing reports" menu (1500).**

AUDITCON displays menu 1580, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-31
Menu 1580: Select Old Audit File



2. **Move the cursor to select the desired audit file, then press** Enter**.**

   AUDITCON displays menu 1581 to display the available filters.

Figure 5-32
Menu 1581: Select Filter

3. **Choose the desired filter and press** Enter**, or press** F10 **to edit a filter.**

   AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and displays the formatted records to your screen. The screen format is as described in “Generating Container Audit Reports” on page 172 (menu 1561).

4. **Use the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer “Yes” to return to menu 1500.**

View Old Audit History

This section describes how to display a listing of the auditor events from an old online audit file to the screen of your workstation.

Prerequisites

Checklist

❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports.” in this chapter.

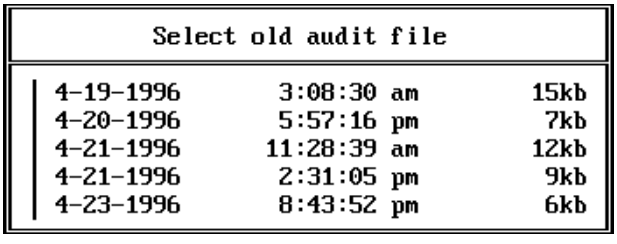
Procedures

Procedure

1. **Choose “View old audit history” from the “Auditing reports” menu (1500).**

   AUDITCON displays menu 1590, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-33
Menu 1590: Select Old Audit File



2. **Move the cursor to select the desired audit file, then press Enter.**

   AUDITCON retrieves records from the current audit file, formats the records, and displays them to your screen. The screen format is as described in “Generating Container Audit Reports” in this chapter (menu 1570).

3. **Use the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer “Yes” to return to menu 1500.**

Database Report Audit File

This section describes how to generate a file containing the user events in the current audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❏ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❏ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the database file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedure

Procedure

1. **Choose “Database report audit file” from the “Auditing reports” menu (1500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 1801 to display the available filters. This includes the files with .ARF extensions in your current directory and a null filter (“_no_filter_”) that will pass all records in the audit file.

Figure 5-34
Menu 1801:Select Filter

3. **To use one of the available filters, choose that filter and press** Enter**.**

AUDITCON also allows you to create a temporary filter, or modify an existing filter, for use in this report. Choose the desired filter, or "_no_filter_", and press F10. Edit the filter as described in "Generating Reports from Offline Audit Files" on page 204.

When you press Esc, you are prompted to discard the changes, save the changes to a filter file, or apply the filter to the current report without saving the changes.

AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.

Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process.

AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait" notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

4. **Exit to DOS and use an appropriate database loading program to insert the audit records into a database for review.**

   See "Format of the Database Output File" on page 203 for a description of the format of the database file.

Database Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file in a format suitable for loading into a database.

Prerequisites

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedures

1. **Choose “Database report audit history” from the “Auditing reports” menu (1500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

   If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

   AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a “Reading file” message in the header area of your screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

3. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

See “Format of the Database Output File” on page 203 for a description of the format of the database file.

Database Report Old Audit File

This section describes how to generate a file containing the user events in an old online audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

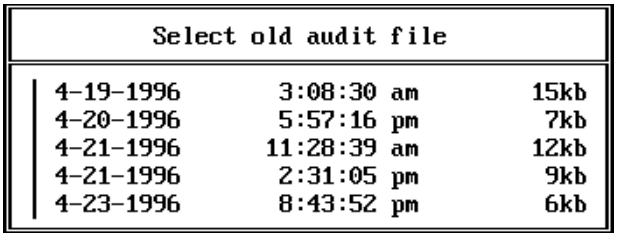
Procedures

Procedure

1. **Choose “Database report old audit file” from the “Auditing reports” menu (1500).**

   AUDITCON displays menu 1820, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-35
Menu 1820: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON displays menu 1822 to display the available filters.

Figure 5-36
Menu 1822: Select Filter

4. **Choose the desired filter and press** Enter**, or press** F10 **to edit a filter.**

   AUDITCON retrieves records from the current audit file, applies the specified filter to those records, formats the filtered records, and writes formatted records to your output file.

   Depending on the size of the audit file and the complexity of your filter, this can be a time consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

5. **Exit to DOS and use an appropriate database loading program to insert the audit records into a database for review.**

   See "Format of the Database Output File" on page 203 for a description of the format of the database file.

Database Report Old Audit History

This section describes how to generate a file containing the auditor events in an old online audit file in a form suitable for loading into a database.

Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29 and the Audit Report Prerequisites in “Generating Container Audit Reports” on page 172.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

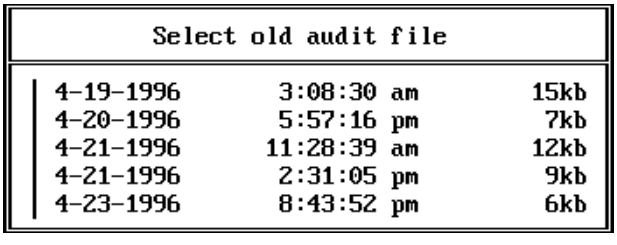
Procedures

Procedure

1. **Choose “Database report old audit history” from the “Auditing reports” menu (1500).**

   AUDITCON displays menu 1830, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-37
Menu 1830: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the output file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you don't specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 1500.

4. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

   See "Format of the Database Output File" on page 203 for a description of the format of the database file.

Format of the Database Output File

Each line in the output file represents a single audit record. Each line consists of a series of comma-separated fields in the following order:

- Time, as hh:mm:ss
- Date, as mm-dd-yyyy
- A "C" to indicate the record came from a container audit trail
- Container object class
- The name of the container where the audit record was generated
- A textual description of the event (for example, "File search")
- The word "event" followed by the numerical event number
- The word "status" followed by the status from the event
- The name of the user for whom the event was generated
- The replica number
- Zero or more pieces of event specific information

This format is suitable to be imported into most databases by specifying that the input is a comma-separated text file.

Generating Reports from Offline Audit Files

In addition to processing online audit files (see “Generating Container Audit Reports” on page 172), AUDITCON also allows you to process offline audit files. These offline files can be stored on the auditor’s workstation, removable media, or even in the auditor’s directory on the server file system.

Files stored in the server file system are considered offline, even if they contain audit data, because the server does not directly manage these files as audit files. Offline audit files are in the same null-compressed, binary format as the server’s audit files described in Appendix A, “Audit File Formats,” on page 267.

This section describes how to process and protect these offline audit files.

Offline Report Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ To process offline audit files, you must either have the Read right to the Audit File object Audit Contents property or have logged in to the audit trail.

AUDITCON controls access to the offline audit file based on the current contents of the Audit File object for that file. Your rights to the Audit File object might be different from your rights when the offline audit file was recorded, so, for example, you might not be able to read an offline audit file that you recorded. This is a constraint imposed by AUDITCON, and not a server access control mechanism. Offline audit files must be protected by the client Trusted Computing Base or (for removable media) by physical protection.

- ❑ You must have previously copied an online audit file from the server to a diskette, your local workstation hard drive, or a network drive. (See “Copy Old Audit File” in this chapter for more information on copying a server's audit files.)

- ❑ You must have access to an offline audit file. You must have at least Read and File Scan rights to access offline audit files on network drives. See your workstation documentation for information on the use of file system rights on your workstation.

Procedure

Procedure

1. **Choose "Reports from old offline file" from the "Available audit options" menu (1101).**

   AUDITCON prompts you for the name of an offline audit file.

   For DOS workstations, the filename can be an absolute DOS pathname (for example, "F:\AUDIT\95FEB15.DAT") or a relative pathname in your current directory (for example, "AUDIT.DAT").

2. **Enter the pathname for the offline audit file. Press** Enter **to open the audit file or** Esc **to return to menu 1600.**

   If AUDITCON cannot open the file, it displays an error message.

   If AUDITCON can open the file, it displays menu 1602, which permits you to select more operations on the offline audit file.

Figure 5-38
Menu 1602: Reports from Old Offline File

```
Reports from old offline file

Edit report filters                1501
Report audit file                  1520
Report audit history               1530
View audit file                    1560
View audit history                 1570
Database report audit file         1800
Database report audit history      1810
```

3. **Choose the desired operation, then press** Enter **to perform that operation.**

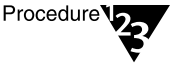
Edit Report Filters

This section describes how to create and edit report filters that you can subsequently use to display specific information that is of interest. There is no distinction between filters for online files and filters for offline files; if you've already created a filter for viewing online audit files, you can use (or modify) that filter for viewing offline audit files.

Prerequisites

❑ See “General Prerequisites” on page 29 and the Offline Report Prerequisites in “Generating Reports from Offline Audit Files” on page 204.

Procedure



1. **Choose “Edit report filters” from the “Reports from old offline files” menu (1602).**

   AUDITCON displays 1501.

2. **Follow the procedures in “Edit Report Filters” on page 176 to create or edit audit report filters.**

Report Audit File

This section describes how to generate a formatted report of the audit records in an offline audit file.

Prerequisites

❑ See "General Prerequisites" on page 29 and the Offline Audit Report Prerequisites in "Report Audit File" on page 184.

Procedure

1. **Choose "Report audit file" from the "Reports from old offline files" menu (1602).**

   AUDITCON displays menu 1520.

2. **Follow the procedures in "Generating Container Audit Reports" on page 172 to generate an audit report for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Report Audit History

This section describes how you can generate an text report of the audit history information in an offline audit file.

Prerequisites

❑ See "General Prerequisites" on page 29 and the Offline Audit Report Prerequisites in "Generating Reports from Offline Audit Files" on page 204.

Procedure

1. **Choose "Report audit history" from the "Reports from old offline files" menu (1602).**

   AUDITCON displays menu 1530, which lists more configuration options.

2. **Follow the procedures in "Report Audit History" on page 186 to generate an text audit history report for an offline audit file.**

References in that section to the “current audit file” should be interpreted as references to an offline audit file.

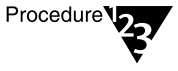
View Audit File

This section describes how you can view (on your workstation screen) audit records from an offline audit file.

Prerequisites

❑ See “General Prerequisites” on page 29 and the Offline Audit Report Prerequisites in “Generating Reports from Offline Audit Files” on page 204.

Procedure



1. **Choose “View audit file” from the “Reports from old offline files” menu (1602).**

   AUDITCON displays menu 1560.

2. **Follow the procedures in “View Audit File” on page 190 to view an offline audit file.**

View Audit History

This section describes how you can view (on your workstation screen) the audit history for an offline audit file.

Prerequisites

❑ See “General Prerequisites” on page 29 and the Offline Audit Report Prerequisites in “Generating Reports from Offline Audit Files” on page 204.

Procedure

1. **Choose “View audit history” from the “Reports from old offline files” menu (1602).**

   AUDITCON displays menu 1570.

2. **Follow the procedures in "View Audit History" on page 193 to view the audit history for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Database Report Audit File

This section describes how to generate a report of the audit records in an offline audit file in a form suitable for loading into a database.

Prerequisites

❑ See "General Prerequisites" on page 29 and the Offline Audit Report Prerequisites in "Generating Reports from Offline Audit Files" on page 204.

Procedure

1. **Choose "Database report audit file" from the "Reports from old offline files" menu (1602).**

   AUDITCON displays menu 1800.

2. **Follow the procedures in "Database Report Audit File" on page 196 to generate an audit report for an offline audit file.**

   References in that section to the "current audit file" should be interpreted as references to an offline audit file.

Database Report Audit History

This section describes how you can generate a report of the audit history information in an offline audit file in a form suitable for loading into a database.

Prerequisites

❑ See "General Prerequisites" on page 29 and the Offline Audit Report Prerequisites in "Generating Reports from Offline Audit Files" on page 204.

Procedure

1. **Choose “Database report audit history” from the “Reports from old offline files” menu (1602).**

   AUDITCON displays menu 1810.

2. **Follow the procedures in “Database Report Audit History” on page 199 to generate a text audit history report for an offline audit file.**

   References in that section to the “current audit file” should be interpreted as references to an offline audit file.

Container Audit File Maintenance

This section describes how you can use AUDITCON to close, copy, delete, and display the server’s old audit files. These mechanisms work only for old audit files (the files maintained online by the server). You cannot perform these operations on offline audit data files. The only operation you can perform on the server’s current audit file is to reset the file, which causes the server to create a new current audit file.

Maintenance of each container audit trail must be performed on a single server which holds a replica of the audit trail. It doesn’t matter which one you choose, but all auditors of the container must use that copy. Failure to use a single copy for maintenance can cause unexpected results and/or loss of configuration changes.

Audit File Maintenance Prerequisites

❑ See “General Prerequisites” on page 29.

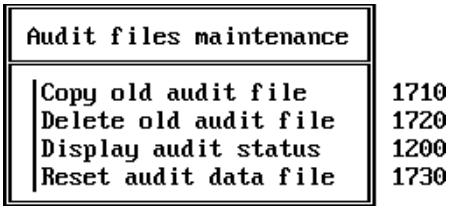
Procedure

1. **Choose “Audit files maintenance” from the “Available audit options” menu (1101).**

2. **Press** Enter**.**

   AUDITCON displays menu 1700, which lists more maintenance options.

Figure 5-39
Menu 1700: Audit Files Maintenance



Copy Old Audit File

This section describes how to copy old online audit files to removable media (for example, diskettes or magnetic tapes), workstation directories, or network drives. The primary reason for copying an audit file is to save the contents of the file before you delete it from the server (see "Delete Old Audit File" on page 213). You might also want to copy an old audit file to removable media to save it for evidence or to keep it for long-term storage.

Prerequisites

Checklist

- ❑ See "General Prerequisites" on page 29.
- ❑ To copy an online audit file, you must either have the Read right to the Audit File object Audit Contents property or have logged in to the audit trail. (To log in to an audit trail, you must enable audit passwords at the server console; this configuration is not permitted in NetWare Enhanced Security facilities.)
- ❑ You must have sufficient rights copy the audit file to a directory. For network directories, you must have at least the Create right. See your client documentation for more information on rights required to create a file on a hard drive or diskette.

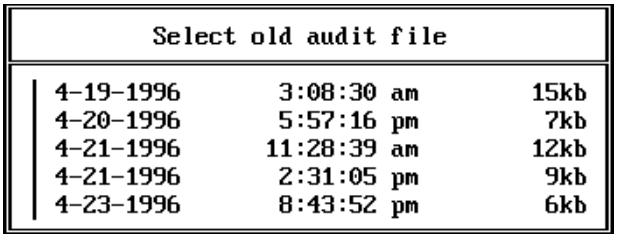
Procedure

Procedure

1. **Choose "Copy old audit file" from the "Audit files maintenance" menu (1700).**

   AUDITCON displays menu 1710, which lists up to 15 old audit files that are maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 5-40
Menu 1710: Select Old Audit File



Note

There is no mechanism for copying the contents of the current audit file. If you want to copy this data, you must first reset the audit data file (see "Reset Audit Data File" on page 214).

You can copy only one file at a time. If you want to copy multiple audit files, perform the steps in this section once for each file.

2. **Move the cursor to select the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the offline audit file.

3. **Enter the filename of the destination audit file and press** Enter**.**

   The pathname must be a DOS pathname on your local workstation, for example, "A:\AUDIT301.DAT", "C:\AUDIT\FILE1.DAT", or "F:\AUDITOR\VOL1\A950224.DAT". If you do not specify a drive letter and directory, AUDITCON will leave the audit file in your current directory. The default pathname is "AUDITOLD.DAT" on your local drive.

   AUDITCON displays a "Please wait" message while it copies the audit file from the server to your offline destination file. When it has copied the file, AUDITCON returns to menu 1700.

4. **If you copy audit files from the server onto your local workstation's file system, you must ensure that the audit data is properly protected by your workstation.**

5. **If you copied the audit file onto removable media (for example, a diskette or tape cartridge), attach a diskette or tape label that shows the server name, volume name, your name, the date, time, and size of the audit file, along with any other specific comments that you feel are important. You must also ensure that the media is physically protected.**

The purpose of this information is to ensure that in the future you can load the medium and generate meaningful audit reports from it.

When backing up old audit files, you must remember to back up the file from each server that holds a replica of the audited container. Otherwise, you can lose some audit records that are stored on some (but not all) copies of the audit file.

One strategy that is commonly used is to set the maximum audit file size so that one audit file will fit on a 1.44 MB diskette. See “Audit Options Configuration” on page 164 for information on setting the audit file size.

The frequency at which you should copy the server's audit files to offline storage depends on how fast your server fills up audit files. If your server archives audit files on a periodic basis (as opposed to filling up the audit file), then you can set the number of audit files to 10 or 15, and copy/remove online audit files once per week without expecting to overflow the number of audit files.

Delete Old Audit File

This section describes how to delete an old audit file from the server’s online storage after you’ve copied the file to offline storage or decided that you do not need to save the file.

When you delete an old container audit file, you must delete the file on each server that holds a replica of the audited container.

Prerequisites

- ❑ See “General Prerequisites” on page 29.
- ❑ To delete an online audit file, you must either have the Write right to the Audit File object Audit Policy property or have logged in to the audit trail. If dual-level passwords are enabled, you must have the level 2 password.

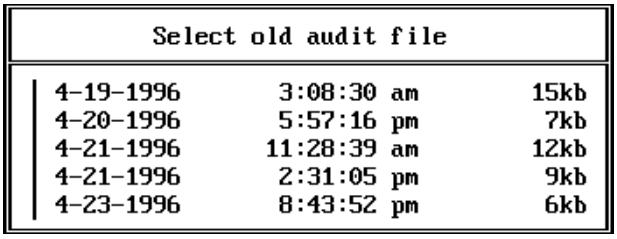
Procedure

1. **Choose “Delete old audit file” from the “Audit files maintenance” menu (1700).**

   AUDITCON displays menu 1720, which lists up to 15 old audit files that are maintained online by the server. The dates and times displayed show when the audit file was created (that is, when it

started accumulating audit events). The old audit files are sorted by date and time (oldest first).

Figure 5-41
Menu 1720: Select Old Audit File



Note

There is no mechanism for deleting the current audit file. If you want to delete the data in the current audit file, you must first reset the audit data file (“Reset Audit Data File” on page 214).

You can only delete one file at a time. If you want to delete multiple audit files, perform the steps in this section once for each file.

2. **Move the cursor to select the desired audit file, then press** Enter**.**

AUDITCON confirms that you want to delete the audit file.

Warning

After you delete an online audit file, there is no way to recover the contents of the file. Do not delete the file unless you are absolutely certain that you will not require the data in the audit file. If there is any doubt, copy the audit file (“Copy Old Audit File” on page 211) to offline storage before you delete the file.

Reset Audit Data File

This section describes how to reset the current audit file. Reset is a manual means of causing the current audit file to be archived, that is, to cause the current audit file to become an old audit file and to establish a new current audit file.

Manual reset might be necessary, for example, if the server stops processing container requests because the volume is in an overflow state. See “Audit Trail Overflow” on page 215 for information on recovering from container overflow.

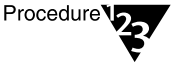
Prerequisites

Checklist

- ❑ See “General Prerequisites” on page 29.

❑ To reset the current audit file, you must either have the Write right to the Audit File object Audit Policy property or have logged in to the audit trail. If dual-level passwords are enabled, you must have the level 2 password.

Procedure



1. **Choose “Reset audit data file” from the “Audit files maintenance” menu (1700).**

   AUDITCON requests confirmation that you want to perform the reset.

2. **Choose “Yes” and press** Enter **to reset the current container audit file.**

Resolving Container Audit Problems

This section describes solutions to potential container audit problems. These include audit trail overflow and synchronization of the container audit files to other NDS partitions, as well as recovery from catastrophic failures.

Audit Trail Overflow

“Preventing Loss of Audit Data” on page 23 describes the potential for audit loss if the configured number of audit files are filled or disk space fills up and the audit trail is improperly configured.

“Audit Options Configuration” on page 164 describes the three overflow configuration options for container audit trails: archive audit file; disable audited events; and disable event recording. The only option that prevents the loss of audit events (from audit overflow situations) is to disable audited events. With this setting, the server disables all audited NDS events when the current audit file has reached the “Audit file maximum size” or the server cannot write the current audit file (for example, out of disk space).

In this overflow state, any event that is preselected for auditing is disabled. For example, if logins are preselected for auditing, any attempt to log in to an object in the container (except for attempts by auditors of the container) would fail.

To recover from the overflow state, an auditor (with the Write right to the container Audit File object Audit Policy property) must reset the current audit trail.

1. Log in to the network as an auditor of the offending container.

2. If you want to save the oldest audit file and you haven't already backed it up, then copy the oldest old audit file to offline storage (for example, a file in the server or workstation or removable media).

3. Reset the current container audit file, as described in "Reset Audit Data File" on page 214. This rolls over the current audit file (to an old audit file), deleting the oldest old audit file, and initializes a new audit file.

4. If you want to save any audit files that you haven't already saved (including the newest of the old audit files), then copy those audit files to offline storage.

Consider the following suggestions to help prevent container overflow:

1. Perform frequent reviews of the status and size of the audit file.

2. If necessary, manually reset the audit file before it overflows.

3. Enable "Automatic audit file archiving" as described in "Audit Options Configuration" on page 164. Set the "Audit file maximum size" large enough and the "Days between audit archives" low enough that the audit file will not overflow. Use caution in setting these parameters to prevent destruction of audit data.

4. Don't over audit.

If the audit trail for a container is full, the auditor's actions (for example, deleting data files, resetting the audit file) might not be audited for that container. In this case, you must keep a manual log of your actions for use when generating a complete history of actions performed on the server. You will be informed via a message from the server to your workstation when this occurs.

When the audit trail is reaches its configured threshold, you will receive the following notification on your workstation screen:

`The audit overflow file for container` *`contname`* `is almost full. Auditors must begin manual auditing now!`

When the audit trail is completely full, you will receive the following notification on your workstation screen:

`The audit overflow file for container` *`contname`* `is full.`

To avoid missing this message, you must not issue the SEND /A=N or SEND /A=P commands (or if using Windows* and the NetWare User Tools, do not disable network warnings), as they would cause these messages to be suppressed.

Container Audit File Replication

Container audit files are replicated by NDS to the servers that hold replicas of the container object. That is, if container LAB1.ENGR.ACME is replicated by NDS onto three different servers, then the audit file for that container will also be replicated onto the same three servers. Replication of container audit files is automatic, and there is no way that you can tell the server to not replicate the audit file, other than to not replicate the audited container.

Replication of container audit files requires disk space on multiple servers. For example, if your container audit trail is configured for 16 audit files (1 current, 15 old) of 1 MB and the container is replicated on three servers, then the audit storage could require as much as 16MB on each server, for a total of 48 MB of disk space.

Records in replicated container audit trails are not necessarily stored in the same order, however, each replica of the audit file will eventually include nearly all of the audited events. In some rare cases (as described in “Generating Container Audit Reports” on page 172) records might be in some instances of the audit trail but not others.

Catastrophic Failure Recovery

This section describes what to do if you have a catastrophic failure, such as

- All copies of the Audit File object describing the container being audited are destroyed (perhaps because of a hard disk failure) and you need to recover the audit state to what it was before the failure
- Volume SYS: on one or more servers holding the audit data are destroyed

In addition, it explains how to handle planned upgrades, such as when a server is upgraded so that volume SYS: (where the container audit data is stored) is moved from a small disk drive to a larger disk drive.

There are several potential losses not addressed here:

- Loss of offline audit data. Your offline audit data (be it stored in server or workstation file systems, or on removable media) should be backed up frequently enough that its loss would not be catastrophic. Because different copies of the container can have different audit data in their audit files, it might be important to create offline copies of all instances of each container audit file.
- Loss of some, but not all, copies of the Audit File object describing the container audit trail due to failure of one or more servers holding an NDS partition. In this case, NDS will automatically use whatever copies are available. If a server configured for the partition is brought back online, it will automatically be updated with the Audit File object information.

There are two major catastrophic failures possible for external audit:

- Loss of all copies of the Audit File object describing the container audit trail. If all copies of the Audit File object are lost (for example, because there only was one copy, and the server it was on suffered a disk failure), then you might be able to recover the Audit File object from a backup of your Directory tree (presuming you have backed up your Directory tree). If so, then you can regain access to the existing online audit data. If not, then no access is possible to the online audit data. You must recreate the container audit trail using the procedures in “Enabling Container

Auditing" on page 152 (including selecting events, audit full actions, and so on).

- Loss of volume SYS: on any server containing the container audit data (for example, because of a disk failure). Because container audit files are stored in an inaccessible directory which cannot be backed up, loss of volume SYS: means that the online audit files (both the current audit file and any old audit files) are lost. You should use AUDITCON to perform regular backups of audit data to avoid loss of online audit data.

  If there is at least one other server with a copy of the container, then when the failed server comes back online it will automatically be updated, and container auditing will automatically resume. If there are no other servers with copies of the container, you must restore the container from an NDS backup and recreate the container audit trail using the procedures described in "Enabling Container Auditing" on page 152.

If you restore a container from an NDS backup, it will come back without auditing. To avoid unaudited actions while you are configuring the audit system, you should take the server offline for the restoration process until the container audit has been reconfigured. To do this, disconnect the server from any networks it is connected to, and attach it to a protected LAN containing only a trusted workstation located in a secure location. Then restore the NDS container from the backup. Use the trusted workstation to run AUDITCON to re-enable container auditing, restoring the previous configuration. Finally, reconnect the server to the standard networks.

If you upgrade volume SYS: (for example, replacing it with a larger disk), that is equivalent to recovery from a catastrophic disk failure. To do an upgrade, you must first back up the old volume, and then restore it on the new disk. This loses all audit data. Therefore, before performing a volume upgrade, you should also back up all container audit data stored on that server. When the upgrade is complete, NDS will automatically cause auditing to resume for those containers with at least one other copy in the network.

Immediacy of Changes

When you modify the container audit trail configuration (for example, to change the maximum size of the audit file or the set of events to be recorded), the change is made both to the Audit Policy property of the Audit File object and to the header of the current audit file in the selected replica of the container.

Both changes will usually occur immediately. From the selected replica, the changes propagate to all other instances of the replica, which again usually happens immediately. However, the effect of the change might not be immediate if one or more of the servers holding the audit data are unavailable to receive the configuration change (for example, because they are down or the network has been split), even though the Audit File object can be modified.

In this case, the delay depends on how long it takes before the two servers can synchronize their NDS replicas. See *NetWare Enhanced Security Administration* for information on how to determine when synchronization occurs.

In addition, if an auditor is performing audit trail management functions, changing the ACL will not affect the auditor's capabilities (either to increase or decrease them). An auditor's rights are recalculated every time he or she restarts AUDITCON and establishes access to an audit trail. To stop the auditor's actions immediately, you should break the auditor's connection to the server using the console MONITOR utility or the CLEAR STATION console command.

chapter 6

Using AUDITCON to Audit External Audit Trails

Chapters 4 and 5 of this manual dealt with the user of the AUDITCON utility to audit server events. NetWare® servers also maintain and protect "external audit trails" that contain client audit records and client audit history.

For an explanation of these external audit trails, see Chapter 1, "Concepts of NetWare Auditing," on page 1 in this manual.

Figure 1-4, Figure 1-5, and Figure 1-6 show the client-server interactions for configuring external audit trails, appending audit records, and reviewing collected audit data. Each client workstation that uses the server's external audit trail must have its own workstation-based audit management tool to configure and manipulate the external audit trail.

AUDITCON can manage external audit trails, but cannot generate reports or view the events stored in those audit trails (except for audit history events). There is no standard with respect to the events that are audited by the workstations or the formats of those audit records.

See the vendor's documentation provided with your client workstation for information on the specific utilities for viewing external audit data.

As shown in Figure 1-4 and Figure 1-6, AUDITCON interacts with the server's external audit trail by sending NCP™ messages to the server. AUDITCON enables auditing by creating an Audit File object for the external audit file and assigning rights to various workstation objects to append audit data to the corresponding audit file.

The workstation object can be linked to the Audit File object by setting the workstation object's Audit File Link property, and the Audit File object can be linked to audited workstations by setting the Audit File object's Audit Link List property (AUDITCON does not set up either the Audit File Link or Audit Link List for external audit trails).

Note that multiple workstations can share a single audit trail and that a workstation can simultaneously support multiple such audit trails.

The external audit trail is protected by configuring the Audit File object to define the NDS™ objects that can append data to the audit file. (See “Create External Audit Trail” on page 228.) Generally, these objects are workstation network trusted computing base partitions. The NDS objects are also defined to read data from the audit file (generally, auditors of those workstations).

Users at client workstations can’t access the external audit files using normal file management NCP programs. AUDITCON does not provide facilities to set up external audit trail protection; you can use NETADMIN or the NetWare Administrator to perform that task.

See your client documentation for information on the availability of NETADMIN and NWADMIN in your client evaluated configuration.

To examine audit data generated by workstations, you can use AUDITCON with a client-specific audit utility. AUDITCON reads the audit data from the external audit trail, displaying the audit history (audit trail management) events.

AUDITCON will also read the workstation-generated audit data from the external audit trail and put it in an ordinary file, where it can then be processed by a client-specific utility that has knowledge of the client audit event formats. AUDITCON can also perform complete backups of external audit files, just as it does for volume and container audit trails.

The specific procedures used to format records from an external audit trail are defined by your client vendor’s audit management tool. If your client workstation uses external audit files to store workstation audit data, refer to your vendor’s trusted facility information for these procedures.

Accessing the External Audit Trail

This section describes how to access the external auditing menu tree and how to select an external audit trail for auditing. Password-based access is not supported for external audit trails. You should have read Chapter 3, "Using the AUDITCON Utility," on page 29, which describes how to run AUDITCON and navigate the menu tree.

Getting Started

When you run AUDITCON, it displays a screen with one of the five "Available audit options" menus. The particular entry menu you see depends only on your current volume and the state of that volume audit trail.

The external auditing state is independent of the state of volume and container auditing. You do not have to enable auditing of a volume or container or have access to a volume or container audit trail to perform external auditing.

Prerequisites

- ❑ See the "General Prerequisites" on page 29.
- ❑ To examine, configure, or modify an external audit trail, you must have the Read right to the Audit File object's Audit Path property.
- ❑ If you are unfamiliar with NDS concepts, review *Guide to NetWare 4 Networks*. If you are unfamiliar with the implementation of your Directory tree, run a graphical utility such as the NetWare Administrator to browse the tree.

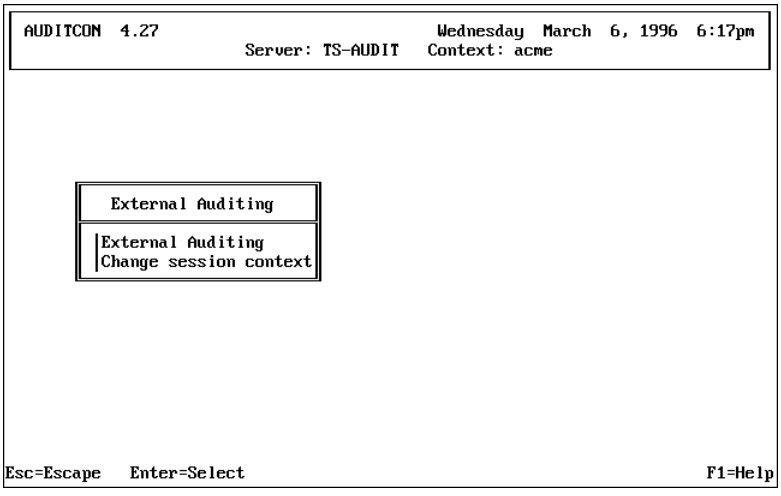
See your client documentation for information on the availability of NETADMIN and NWADMIN in your client evaluated configuration.

Procedure

1. **Choose "External auditing" from the initial "Available audit options" menu (101, 102, or 103).**
2. **Press** Enter**.**

   AUDITCON displays menu 2000, which shows the full screen for external audit trail management. The second line of the header defines the NDS context where you are working.

Figure 6-1
Menu 2000: AUDITCON Full Screen for External Audit Trail



Warning

The top line of the screen only shows the session (container name), and does not show the name of the external audit trail being manipulated. You must remember which external audit trail is in use to ensure that your actions are as intended.

Change Session Context

To perform external audit management, your session context (shown in the second line of the header area) must point to the external audit trail.

AUDITCON provides two methods of changing your NDS session context.

- The first method, “Change session context”, described in this section, allows you to type in the explicit context for the external audit trail’s Audit File object that you want to audit. This might be the preferred method if your network has many external Audit File objects and you know exactly which Audit File object you want to audit
- The second method, described in “External Auditing” on page 225, permits you to browse through the NDS tree and select an Audit File object for auditing. This is generally the preferred method because you can select an Audit File object and begin auditing that external audit trail in a single operation.

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.
- ❑ You do not have to have any rights to the NDS Audit File object to set the session context.

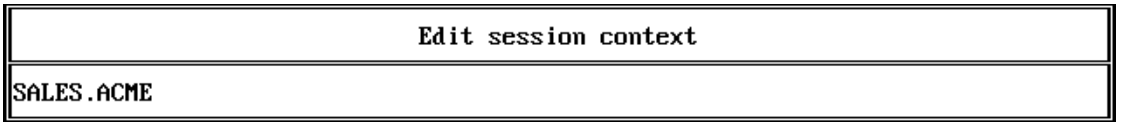
Procedure

Procedure

1. **To define a different external audit trail for auditing, choose “Change session context” in the “External auditing” menu (2000) and press** Enter**.**

   AUDITCON displays menu 2001, which allows you to edit the current session context

Figure 6-2
Menu 2001: Edit Session Context



2. **Edit the current session context by backspacing and typing over the existing container name or pressing** Home **and inserting text at the beginning of the line.**
3. **When you are done, press** Enter **to change context to the specified external audit trail object.**

   If the Audit File object does not exist, AUDITCON displays an error report.

4. **Return to menu 2000, then choose “External auditing” to begin auditing the Audit File object.**

Warning

AUDITCON does not display the name of the currently selected external audit trail on the screen. It is your responsibility to remember which audit trail you are working on at all times.

External Auditing

This section describes the second method of changing your NDS session context that was referred to in “Change Session Context” on

page 224. This option allows you to browse the Directory tree to select an Audit File object for auditing, then displays a menu that allows you to begin auditing that external audit trail. If you have already selected the container, then you do not need to browse the Directory tree.

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.
- ❑ To browse the Directory tree for external audit trails, you must have the Browse right to the container that the Audit File object corresponding to the external audit trail is in. Otherwise, AUDITCON will not be able to find the Audit File object.

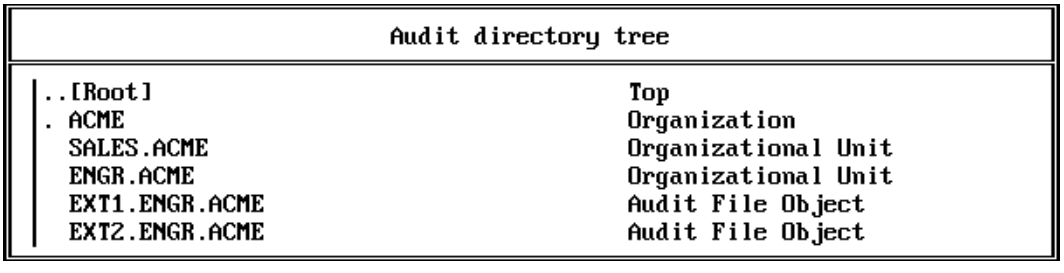
Procedure

Procedure

1. **Choose “External auditing” in the “External auditing” menu (2000) and press** Enter**.**

   AUDITCON displays menu 2010, which allows you to iteratively browse the Directory tree to select an external Audit File object for auditing.

Figure 6-3
Menu 2010: Audit Directory Tree



AUDITCON displays the parent of the current container (in this case, “[Root]”, indicated by “..”), the current container (in this case, “ACME”, indicated by “.”), any containers within the current container (in this case, “SALES.ACME” and “ENGR.ACME”), and any external Audit File objects within the current container (in this case, “EXT1.ACME” and “EXT2.ACME”).

Note

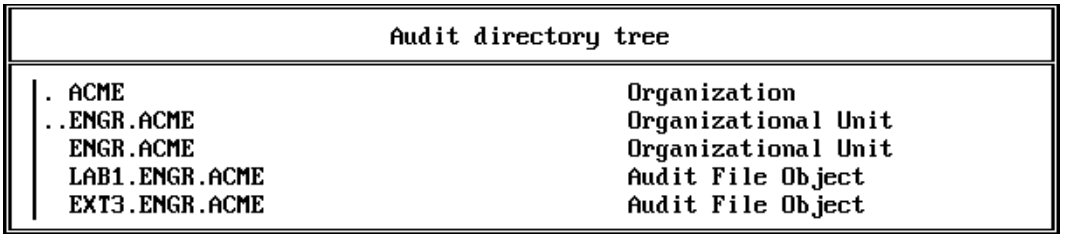
AUDITCON displays as “external audit trails” those Audit File objects that have the Audit Type property set to “External”. If your Audit File object was

created with a utility that did not set the Audit Type property to “External”, then AUDITCON will be unable to locate it, and you will be unable to manage it.

2. **If the menu does not show the external audit trail you want to audit, keep choosing the nearest ancestor and pressing** Enter **until AUDITCON shows the desired external Audit File object.**

   For example, if you want to audit “EXT3.ENGR.ACME”, which is not shown in menu 2010, you would first select “ENGR.ACME”. AUDITCON changes the session context and displays menu 2010-Updated.

Figure 6-4
Menu 2010-Updated: Audit Directory Tree



3. **Move the cursor to the desired external Audit File object, and press** F10 **to review the external audit trail or press** Enter **to display menu 2010 with the new session context. From 2010 you can select the current object for auditing.**

   AUDITCON now changes your NDS context to the selected external audit trail, and updates the context field in the display header area to show the name of the container where that Audit File Object is found.

Warning

AUDITCON does not display the name of the currently selected external audit trail on the screen. It is your responsibility to remember which audit trail you are working on at all times.

If, instead of using an existing external audit trail, you want to create a new audit external audit trail, you should select the container as shown above. Instead of pressing F10 to select an existing Audit File object, press Insert.

Create External Audit Trail

Unlike volume or container audit trails, external audit trails are not created automatically by enabling auditing. Rather, you must use AUDITCON to create a new Audit File object.

AUDITCON will establish a default configuration for the new Audit File object, including setting up the Audit Path property of the Audit File object to point to a volume where the external audit data will be stored. However, AUDITCON won't set up the Audit Link List property of the Audit File object to point to other objects (for example, workstations) that might generate audit data, nor will it set up the Audit File Link property of the other objects to point to the Audit File object.

If your client vendor supplies a tool to set up the Audit Link List and Audit File Link properties, it is a good idea to use it to assist in the maintenance of your audit trail. However, it is not necessary to set these properties, and if you do not set them it will not have any negative impact on performance or security. NETADMIN and NetWare Administrator will not delete an Audit File object if it has a non-empty Audit Link List property.

NetWare does not impose any limits on the number of external audit trails you can have. Consult your client documentation for guidance on how to determine how many external audit trails you need, and how they should be managed. Note that AUDITCON does not provide any means for merging records from multiple external audit trails, so it is best not to create too many different trails which would require manual correlation.

If you have more than one type of client that uses external audit trails (that is, from two different workstation vendors), you should not allow them to insert their audit records into the same audit trail. Although audit records are identified as to the vendor that created them, post-processing software might not include facilities to sort out the different vendor record types.

Depending on your client architecture, it might be important what container the Audit File objects are stored in, and what volume holds the actual audit data. See your client documentation for any such restrictions.

Creating the external audit trail consists of selecting the name of the Audit File object and selecting the volume and server where the Audit File object will be stored.

Once the Audit File object is created, you can use a tool such as NETADMIN or NetWare Administrator to set NDS rights to allow auditors access to the Audit File object (and the corresponding audit data) for management purposes and to allow clients to append to the audit trail. See “Controlling Access to Online Audit Data” on page 17 for a description of the rights needed for each of these purposes.

Prerequisites

- ❑ See the “General Prerequisites” on page 29.
- ❑ To browse the Directory tree for containers to place the new external audit trail, you must have the Browse right to the container that the Audit File object corresponding to the external audit trail will be placed in. You also need the Browse right for the containers (NetWare Server object and Volume object) where the external audit data will be stored.
- ❑ You must also have the Create (or Supervisor) right to the container where the new Audit File object will be placed.

Procedure

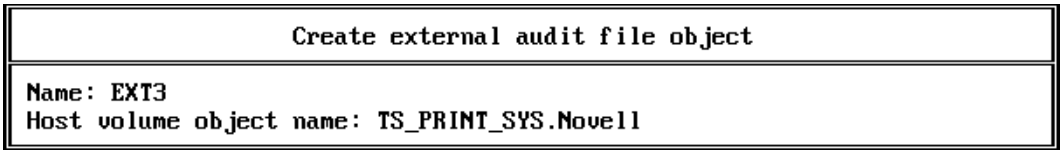
1. **Follow the instructions in “External Auditing” on page 225 to choose a container, and then press** Insert**.**
2. **Type the common name of the external Audit File Object you want to create (for example, EXT3) in the “Name” field, and press** Enter**.**

   Do not enter the distinguished object name. (For an explanation of “common” and “distinguished” names, see the section “Understanding How Network Resources Are Accessed” in *Guide to NetWare 4 NetWorks*.)

   AUDITCON now displays a list of available volume objects on which the files that collect auditing data can be placed.
3. **Move the cursor to the desired volume, and press** F10 **to select it.**

   The menu will now appear as in menu 2061.

Figure 6-5
Menu 2061: Create External Audit File Object



4. **Press** F10 **to create the Audit File object or** Esc **if you don't want to create the object.**

   If you press F10, AUDITCON creates the Audit File object in the specified container and the external audit data files in the specified server.

   The external audit trail is now enabled. AUDITCON will update the screen to show the newly created external audit trail at the top, and will place you in menu 2101.

Top-level Menu

After you've selected a specific container for auditing, AUDITCON selects the screen to display depending on

- Whether you have at least Read or Write rights to the Audit Contents or Audit Policy attribute of the Audit File object
- Whether auditing is enabled for the external audit trail

Table 6-1 summarizes the algorithm AUDITCON uses to determine which screen to display.

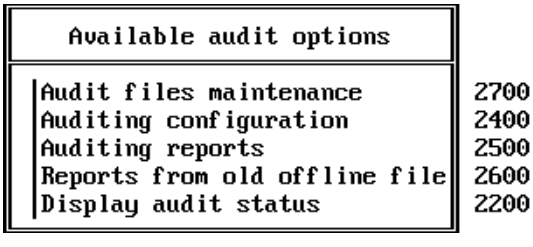
Table 6-1
External Audit Trail Entry Screens

Sufficient Rights	Container Audit Enabled	Screen
Yes	Yes	Menu 2101
Yes	No	“Enable External Auditing” displayed as the only option
No	Yes	Error message
No	No	Error message

The three top-level “Available audit options” menus for external auditing are summarized, as follows.

Menu 2101: AUDITCON displays this menu when the auditor has NDS rights to the selected external audit trail.

Figure 6-6
Menu 2101: Available Audit Options



When the selected external audit trail is not enabled for auditing, this screen displays “Enable External Auditing” as the only option.

When you do not have rights to access the audit trail, an error report displays.

Displaying External Audit Trail Status

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.
- ❑ You must have Read or Write rights to the Audit File object Audit Policy property or Read or Write rights to the Audit File object Audit Contents property to display the external audit trail audit status.

Procedure

Procedure

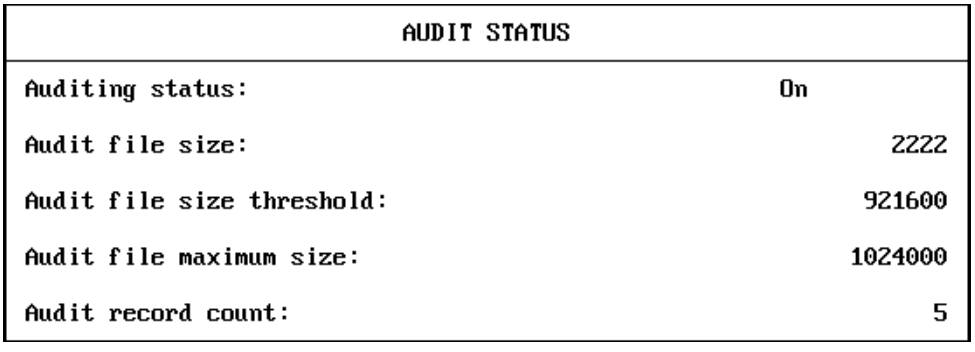
1. **Choose “Display Audit Status” in menu 2101.**

   AUDITCON then displays menu 2200.

   You can invoke this display from various other places in the container audit menu tree. This is a read-only display that presents the audit status for your current external audit trail.

2. **Press** Esc **to return to the calling menu.**

Figure 6-7
Menu 2200: Audit Status



The audit status displays the following status information for the current container audit trail:

Audit Status Information	Description
Auditing status	Shows as “On” if auditing is enabled for the selected external audit trail, or “Off” if auditing is not enabled.

Audit Status Information	Description
Audit file size	Shows the size, in bytes, of the current external audit file.
Audit file size threshold	Shows the configured size at which the server sends warning messages to the server console and system log file.
Audit file maximum size	Defines the nominal maximum size for the audit file.
Audit record count	Defines the number of audit records in the current audit file.

This display does not define the complete status of a external audit trail. See“Changing an External Audit Trail Configuration” on page 234 for more information on viewing and setting the audit configuration.

Enabling External Auditing

When you create an Audit File object for external auditing, AUDITCON enables the external audit trail. This Audit File object remains in place when you disable auditing, and can be re-enabled as follows.

Prerequisites

- ❑ See the “General Prerequisites” on page 29.
- ❑ You must have Write (or Supervisor) object rights to the Audit Policy object of the external audit trail's Audit File object.

Procedure

1. **Run AUDITCON at a trusted workstation.**
2. **Choose the desired external audit trail to be audited, as described in “Create External Audit Trail” on page 228.**
3. **To enable auditing of the external audit trail, choose the “Enable external auditing” option in the “Available audit options” menu.**

This option appears only when auditing is not already enabled for the external audit trail.

4. **Choose "Yes" to re-enable auditing when AUDITCON asks you to confirm that you want to enable auditing for the current external audit trail.**

   AUDITCON will display menu 2101.

Changing an External Audit Trail Configuration

This section describes how you can use AUDITCON's external audit trail configuration menu to define how audit files are handled (size, threshold, automatic archive, and recovery from audit file overflow).

Auditing Configuration Prerequisites

Checklist

- ❑ See the "General Prerequisites" on page 29.
- ❑ You must have the Write right to the Audit Policy property of the Audit File object for which you want to change the configuration.
- ❑ Determine which actions you want to perform (for example, how large you want the audit file to be) before you run AUDITCON.

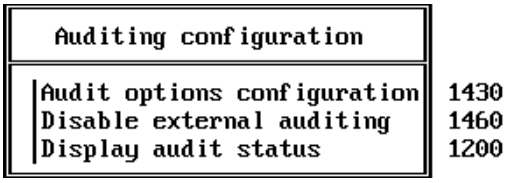
Procedure

Procedure

1. **Choose "Auditing Configuration" from the "Available audit options" menu (2101).**

   AUDITCON displays menu 2400, which lists more configuration options.

Figure 6-8
Menu 2400: Auditing Configuration



2. **Choose the desired configuration option, and press** Enter**.**

   These configuration submenus are addressed in the following sections.

Warning

When you make changes to the external audit configuration, you might receive a message that AUDITCON was unable to update the Audit File object. If this occurs, it is possible that your configuration changes could be lost.

Audit Options Configuration

Prerequisites

Checklist

❑ See the “General Prerequisites” on page 29 and “Changing an External Audit Trail Configuration” on page 234.

Procedure

Procedure

1. Choose “Audit options configuration” from the “Auditing configuration” menu (2400).

AUDITCON displays menu 2430, which defines the current audit configuration for the external audit trail.

Figure 6-9
Menu 2430: Select Audit Configuration

```
                    Audit configuration

Audit file maximum size:                          1024000
Audit file threshold size:                         921600
Audit overflow file size:                          102400
Automatic audit file archiving:                        No
Days between audit archives (1-255):
Hour of day to archive (0-23):
Number of old audit files to keep (1-15):              15
Allow concurrent auditor logins:                       No
Broadcast errors to all users:                         No
 Error recovery options for audit file full
Archive audit file:                                    No
Reject audit records:                                 Yes
Minutes between warning messages:                       3
```

The following list describes the available configuration parameters for external audit trails. The first nine parameters (“Audit file maximum size” through “Broadcast errors to all users”) have the same meaning as for volume auditing.

For more information on these parameters, refer to the description of the corresponding volume configuration parameters in “Audit Options Configuration” on page 70.

Warning

When computing the overflow audit file size (as described in “Audit Options Configuration” on page 70) for an external audit trail, you must use the value for the number of service processes on the server where the audit data is stored.

The server provides two options for handling external audit file overflow. The options are: “Archive audit file” and “Reject audit records.”

Table 6-2
Overflow Options

Overflow option	Description
Archive audit file	With this setting, the server archives the current audit file and creates a new audit file. If necessary (because the maximum number of old online audit files already exists), the server deletes the oldest of the old online audit files. This option is not recommended for use in C2 networks, because it can result in audit data being lost.
Reject audit records	With this setting, the server refuses to accept additional externally generated audit records when the current audit file has reached the “Audit file maximum size” or the server cannot write the current audit file (for example, out of disk space). The server does not attempt to roll over to a new audit file, even if audit files and disk space are available. To recover, you must reset the current audit file as described in “Reset Audit Data File” on page 260. This is the only overflow option that guarantees that you will not lose audit data. Consequently, if collecting audit data is important (such as in a C2 network), then you should use this setting, even thought it might inconvenience users.
Minutes between warning messages	The server sends warnings to the console at this frequency if the audit file is full and the overflow option is configured to either “Disable record submission” or “Reject audit records”.

2. Enter the new configuration value in the field you want to change.

For numeric fields, type the new value over the old value and press Enter. For “Yes / No” fields, type “Y” or “N.”

Depending upon your change, the server might modify other values on the configuration screen. For example, if you set “Automatic audit file archiving” to “No”, the server will blank out

the entries for “Days between audit archives” and “Hour of day to archive.”

3. **Review the settings on the current screen and change as required.**

4. **Press** Esc **to exit the menu.**

Audit files consume disk resources that might be needed by other users. Before you define the number and size of audit files, discuss your projected disk space requirements with an administrator for the server.

Disable an External Audit Trail

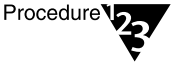
When you disable an external audit trail, you stop the server from accepting or recording audit events to the external audit file, but you do not delete the Audit File object or the audit files. The Audit File object remains in effect and is reused (to provide an initial configuration) if you re-enable auditing for the external audit trail.

After external auditing has been disabled, it can be re-enabled using the Enable External Auditing menu (see “Enabling External Auditing” on page 233).

Prerequisites

❑ See the “General Prerequisites” on page 29 and “Changing an External Audit Trail Configuration” on page 234.

Procedure



1. **Choose “Disable external audit trail” from the “Auditing configuration” menu (2400).**

   AUDITCON asks you to confirm that you want to disable auditing for the external audit trail.

2. **Choose “Yes” and press** Enter **to disable auditing, or “No” to continue auditing.**

   AUDITCON returns to menu 2010.

Generating External Audit Trail Reports

AUDITCON allows you to process online and offline audit files to extract and review the information the server has collected for you. Processing consists of displaying audit information on the AUDITCON screen (viewing) and generating printable reports (printing).

This section describes how to process online audit files, that is, the current audit file or old audit files that have been archived (rolled over) by the server but are still maintained as audit files by the server. See “Generating Reports from Offline Audit Files” on page 252 for information on how to process offline audit files.

For external audit, textual audit reports are provided only for audit history (management) records. For this reason, there is no post-selection filtering capability provided. To see the externally generated audit records, you must store them into a file (using the “Report audit file” or “Report old audit file” options) and then post-process them with a client-specific audit utility.

Audit Report Prerequisites

- ❑ See the “General Prerequisites” on page 29.
- ❑ To process online audit files, you must have the Read right to the Audit File object Audit Contents property.
- ❑ You must have the ability to create new (temporary) files in the directory you were in when you started AUDITCON, and there must be sufficient disk space on that volume. These temporary files hold the audit data as it is extracted from the audit trail.

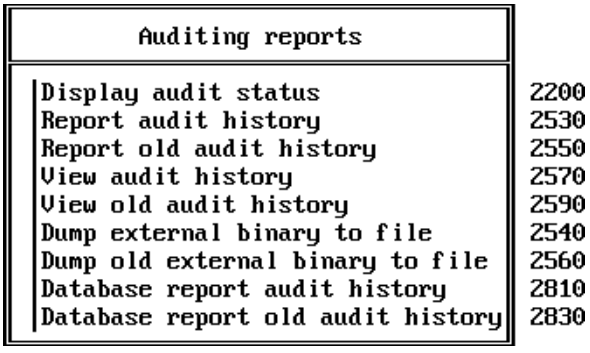
Because AUDITCON places temporary files in the directory you were in when you started AUDITCON, and these temporary files contain audit data, you must not generate any reports unless your current directory is protected from access by users who are not authorized to see audit data.

Procedure

1. **Choose “Auditing reports” from the “Available audit options” menu (2101).**

   AUDITCON displays menu 2500.

Figure 6-10
Menu 2500: Auditing Reports



2. Choose the desired auditing report option, and press Enter**.**

You have several options available for creating and viewing reports from the records in audit files:

- You can process audit history records from the current audit file (for example, “Report audit history”) or an old audit file (for example, “Report old audit history”). References to old audit files explicitly indicate operations on one of the server’s old audit files, while the other operations are implicit on the current audit file.
- You can direct output to your AUDITCON screen (for example, “View audit history”) or send the output to a file on your workstation or a directory on the server (for example, “Report audit history file”). For external auditing, only history records can be viewed.
- You can see the audit history records (for example, “Report audit history”) or cause storage of the externally generated audit records (for example, “Dump external binary to file”).
- You can cause reports to be generated as text (for example, “Report audit history”) or in a form suitable for loading into a database (for example, “Database report audit history”). For external auditing, only history records can be written in a database-loadable format.

These options are addressed in the following sections.

Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file.

The procedures described in this section allow you to generate audit history report files on your local workstation. See your client documentation for details on how to use your workstation's security mechanisms to protect these files.

Prerequisites

- ❑ See the "General Prerequisites" on page 29 and the "Audit Report Prerequisites" on page 238.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedure

1. **Choose "Report audit history" from the "Auditing reports" menu (2500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

3. **To review the contents of your report, exit to DOS and either print or use an editor.**

Dump External Binary to File

This section describes how to generate a binary version of the externally generated events in the current audit file. You cannot directly print the server's audit files because

- The server's audit files are not directly accessible to network clients
- The server's audit files are stored in a compressed format

Once you have the stored binary version of the audit data, you should use a client-specific tool to generate textual versions of the audit data.

In addition, post-selection of the audit records is done with the client-specific tool. See your client documentation for instructions on how to manipulate the binary data.

The audit file report contains audit records that must be protected. You must use appropriate workstation or server protections to protect against access to the file by unauthorized individuals.

The current audit file is a "work in progress." As such, a report that is generated on the current audit file might not be the same as a subsequent report generated on the same file.

Note that storing external audit data (described here) is not the same as making a complete copy of an audit file (as described in "Copy Old Audit File" on page 257). They differ in two ways:

- Copies of audit files have null compression, but stored external audit files have nulls expanded.
- Copies of audit files include both audit history records and externally generated audit records, but stored external audit files only contain externally generated audit records.

Each record in the stored external audit file consists of an external audit record header and client-specific audit data (as described in Appendix A, "Audit File Formats," on page 267).

Prerequisites

- ❑ See the “General Prerequisites” on page 29 and the “Audit Report Prerequisites” on page 238.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedure

1. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

2. **Choose “Dump External Binary to File” from the “Auditing reports” menu (2500).**

   AUDITCON prompts you for the name of the output file.

   If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

   AUDITCON retrieves records from the current audit file and writes unformatted records to your output file. Depending on the size of the audit file, this can be a time consuming process. AUDITCON displays a “Reading file” message in the header area of your screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

3. **To review the contents of your report, exit to DOS and use a client-specific tool to examine the audit data.**

Report Old Audit History

This section describes how to generate a formatted text version of the auditor events in an old online audit file.

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29 and “Audit Report Prerequisites” on page 238.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

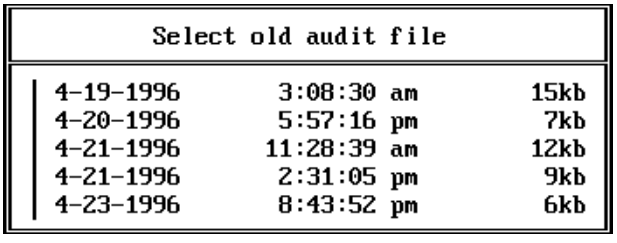
Procedure

Procedure

1. **Choose “Report old audit history” from the “Auditing reports” menu (2500).**

   AUDITCON displays menu 2550, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 6-11
Menu 2550: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

4. **To review the contents of your report, exit to DOS and either print or use an editor.**

Dump Old External Binary to File

This section describes how to generate a binary version of the externally generated events in an old audit file. You cannot directly print the server's audit files, because the server's audit files are not directly accessible to network clients and the server's audit files are stored in a compressed format.

Once you have the stored binary version of the audit data, you should use a client-specific tool to generate textual versions of the audit data. In addition, post-selection of the audit records is done with the client-specific tool. See your client documentation for instructions on how to manipulate the binary data.

The audit file report contains audit records that must be protected. You must use appropriate workstation or server protections to protect against access to the file by unauthorized individuals.

Note that storing external audit data (described here) is not the same as making a complete copy of an audit file (as described in "Copy Old Audit File" on page 257). The two differ in two ways:

- Copies of audit files include both audit history records and externally generated audit records, but stored external audit files only contain externally generated audit records.
- Copies of audit files have null compression, but stored external audit files have nulls expanded.

Each record in the stored external audit file consists of an external audit record header and client-specific audit data (as described in Appendix A, “Audit File Formats,” on page 267).

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29 and “Audit Report Prerequisites” on page 238.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least Create rights on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

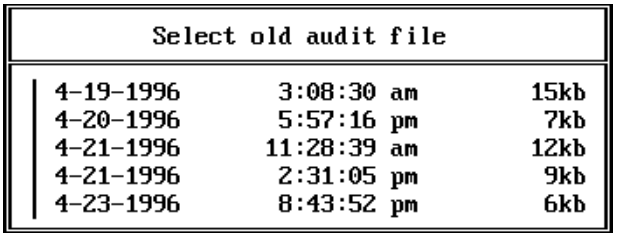
Procedure

Procedure

1. **Choose “Dump Old External Binary to File” from the “Auditing reports” menu (2500).**

   AUDITCON displays menu 2560, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events)

Figure 6-12
Menu 2560: Select Old Audit File



2. **Move the cursor to choose the desired audit file and press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the selected old audit file and writes unformatted records to your output file. Depending on the size of the audit file, this can be a time consuming process. AUDITCON displays a "Reading file" message in the header area of your screen and a "Please wait ..." notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

4. **To review the contents of your report, exit to DOS and use a client-specific tool to examine the audit data.**

View Audit History

This section describes how to display a listing of the auditor events on the screen of your workstation.

Prerequisites

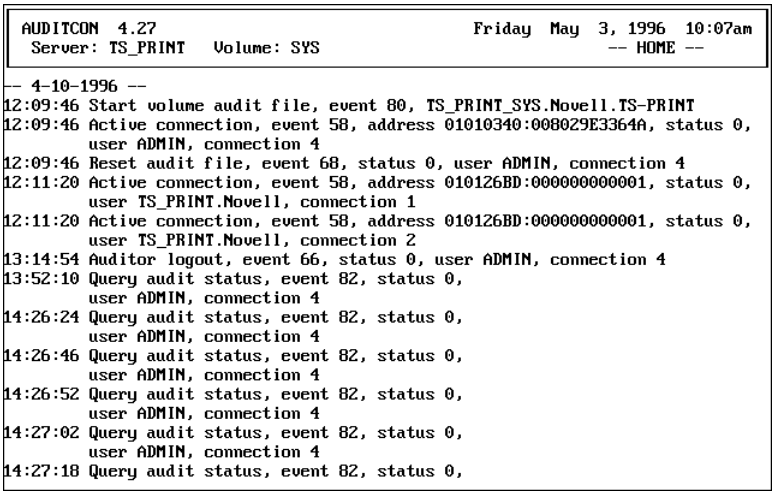
❑ See the "General Prerequisites" on page 29 and "Audit Report Prerequisites" on page 238.

Procedure

1. **Choose "View audit history" from the "Auditing reports" menu (2500).**

   AUDITCON reads the current audit file and displays screen 2570, the first screen of audit history events.

Figure 6-13
Menu 2570: Audit History Events



```
AUDITCON  4.27                                  Friday  May  3, 1996  10:07am
 Server: TS_PRINT   Volume: SYS                                  -- HOME --

-- 4-10-1996 --
12:09:46 Start volume audit file, event 80, TS_PRINT_SYS.Novell.TS-PRINT
12:09:46 Active connection, event 58, address 01010340:0080Z9E3364A, status 0,
         user ADMIN, connection 4
12:09:46 Reset audit file, event 68, status 0, user ADMIN, connection 4
12:11:20 Active connection, event 58, address 010126BD:000000000001, status 0,
         user TS_PRINT.Novell, connection 1
12:11:20 Active connection, event 58, address 010126BD:000000000001, status 0,
         user TS_PRINT.Novell, connection 2
13:14:54 Auditor logout, event 66, status 0, user ADMIN, connection 4
13:52:10 Query audit status, event 82, status 0,
         user ADMIN, connection 4
14:26:24 Query audit status, event 82, status 0,
         user ADMIN, connection 4
14:26:46 Query audit status, event 82, status 0,
         user ADMIN, connection 4
14:26:52 Query audit status, event 82, status 0,
         user ADMIN, connection 4
14:27:02 Query audit status, event 82, status 0,
         user ADMIN, connection 4
14:27:18 Query audit status, event 82, status 0,
```

2. **Press the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer "Yes" to return to menu 2500.**

Note

The "Auditor login" event means that an auditor began accessing the audit file, while the "Auditor logout" event means that an auditor ceased accessing the access file. These events do not indicate user logins or logouts.

View Old Audit History

This section describes how to display a listing of the auditor events from an old online audit file to the screen of your workstation.

Prerequisites

Checklist

❑ See the "General Prerequisites" on page 29 and "Auditing Configuration Prerequisites" on page 234.

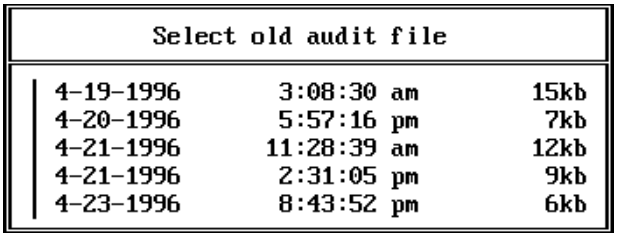
Procedure

Procedure

1. **Choose "View old audit history" from the "Auditing reports" menu (2500).**

AUDITCON displays menu 2590, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 6-14
Menu 2590: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON retrieves records from the current audit file, formats the records, and displays them to your screen (menu 2570).

3. **Press the** Home**,** End**,** Page Up**,** Page Down**, and arrow keys to move through the display. When you are finished, press** Esc **and answer "Yes" to return to menu 2500.**

Database Report Audit History

This section describes how to generate a formatted text version of the auditor events in the current audit file in a format suitable for loading into a database.

Prerequisites

Checklist

- ❑ See the "General Prerequisites" on page 29 and "Audit Report Prerequisites" on page 238.
- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

Procedure

1. **Choose “Database report audit history” from the “Auditing reports” menu (2500).**

   AUDITCON prompts you for the name of the output file.

2. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a “Reading file” message in the header area of your screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

3. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

   See “Format of the Database Output File” on page 251 in this chapter for a description of the format of the database file.

Database Report Old Audit History

This section describes how to generate a file containing the auditor events in an old online audit file in a form suitable for loading into a database.

Prerequisites

❑ See the “General Prerequisites” on page 29 and “Auditing Configuration Prerequisites” on page 234.

- ❑ You must have rights to the directory where you intend to create the output file. For a network directory on the server, you must have at least the Create right on the directory to create the file and [RWCEMF] rights to manage the file after you create it. If you are creating the report file on your local workstation, see your workstation documentation for information on using the workstation's access control mechanisms to protect your files.

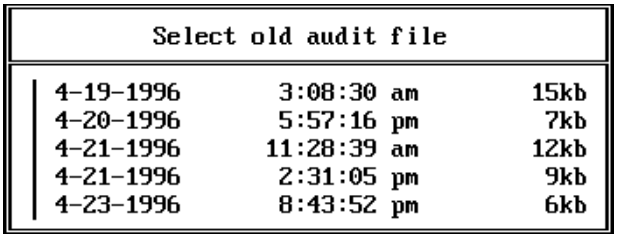
Procedure

Procedure

1. **Choose "Database report old audit history" from the "Auditing reports" menu (2500).**

   AUDITCON displays menu 2830, which lists up to 15 old audit files that are still maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 6-15
Menu 2830: Select Old Audit File



2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON prompts you for the name of the output file.

3. **Enter the pathname for the file and press** Enter**.**

   AUDITCON attempts to create the file and displays an error screen if it cannot.

Note

If you do not specify a complete pathname, including the drive letter, AUDITCON leaves the report on your current drive. The safest approach is to specify the full pathname for your output file.

AUDITCON retrieves records from the current audit file, formats the records, and writes them to your output file. AUDITCON displays a "Reading file" message in the header area of your

screen and a “Please wait ...” notification in the menu area. When it is finished, AUDITCON returns to menu 2500.

4. **Exit to DOS and use an appropriate database loading program to insert the audit history records into a database for review.**

   See “Format of the Database Output File” on page 251 and Appendix A, “Audit File Formats,” on page 267 for a description of the format of the database file.

Format of the Database Output File

Each line in the output file represents a single audit record. Each line consists of a series of comma-separated fields in the following order:

- Time, as hh:mm:ss
- Date, as mm-dd-yyyy
- An “E” to indicate the record came from an external audit trail
- The name of the external audit trail where the audit record was generated
- Container object class
- A textual description of the event (for example, “Write audit config hdr”)
- The word “event” followed by the numerical event number
- The word “status” followed by the status from the event
- The name of the user for whom the event was generated
- The replica number
- Zero or more pieces of event specific information

This format is suitable to be imported into most databases by specifying that the input is a comma separated text file.

Generating Reports from Offline Audit Files

In addition to processing online audit files, AUDITCON also allows you to process offline audit files. These offline files can be stored on the auditor's workstation, removable media, or even in the auditor's directory on the server file system.

Files stored in the server file system are considered offline, even if they contain audit data, because the server does not directly manage these files as audit files.

Offline audit files are in the same null-compressed, binary format as the server's audit files described in Appendix A, "Audit File Formats," on page 267.

This section describes how to process and protect these offline audit files.

Offline Report Prerequisites

- ❑ See the "General Prerequisites" on page 29.
- ❑ To process offline audit files, you must have the Read right to the Audit File object Audit Contents property.

AUDITCON controls access to the offline audit file based on the current contents of the Audit File object for that file. Note that your rights to the Audit File object might be different from your rights when the offline audit file was recorded, so, for example, you might not be able to read an offline audit file that you recorded. Note also that this is a constraint imposed by AUDITCON, and not a server access control mechanism. Offline audit files must be protected by the client TCB or (for removable media) by physical protection.

- ❑ You must have previously copied an online audit file from the server to a diskette, your local workstation hard drive, or a network drive. See "Copy Old Audit File" on page 257.
- ❑ You must have access to an offline audit file. You must have at least Read and File Scan rights to access offline audit files on network drives. See your workstation documentation for information on the use of file system rights on your workstation.

Procedure

Procedure

1. **Choose "Reports from old offline file" from the "Available audit options" menu (2101).**

   AUDITCON prompts you for the name of an offline audit file.

   For DOS workstations, the file name can be an absolute DOS pathname (for example, "F:\AUDIT\95FEB15.DAT") or a relative pathname in your current directory (for example, "AUDIT.DAT").

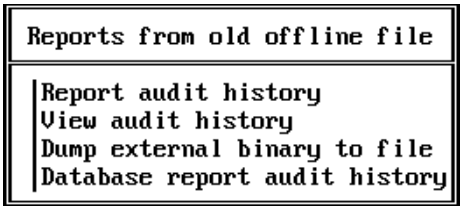
2. **Enter the pathname for the offline audit file.**

3. **Press** Enter **to open the audit file, or** Esc **to return to menu 2600.**

   If AUDITCON cannot open the file, it displays an error message.

   If AUDITCON can open the file, it displays menu 2602, which permits you to select more operations on the offline audit file.

Figure 6-16
Menu 2602: Reports from Old Offline File



4. **Choose the desired operation, then press** Enter **to perform that operation.**

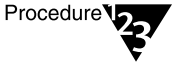
Report Audit History

This section describes how you can generate a text report of the audit history information in an offline audit file.

Prerequisites

❑ See the “General Prerequisites” on page 29 and “Offline Report Prerequisites” on page 252.

Procedure



1. **Choose “Report audit history” from the “Reports from old offline files” menu (2602).**

   AUDITCON displays menu 2530, which lists more configuration options.

2. **Follow the procedures in “Report Audit History” on page 240 to generate a text audit history report for an offline audit file.**

   Interpret references to the “current audit file” as references to an offline audit file.

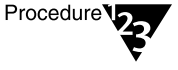
Dump External Binary to File

This section describes how you can generate a binary version of the external audit records in an offline audit file. Use a client-specific utility to convert the binary audit records into a text form.

Prerequisites

❑ See the “General Prerequisites” on page 29 and “Offline Report Prerequisites” on page 252.

Procedure



1. **Choose “Dump external binary to file” from the “Reports from old offline files” menu (2602).**

   AUDITCON displays menu 2540, which lists more configuration options.

2. **Follow the procedures in "Generating External Audit Trail Reports" on page 238 to generate a text audit history report for an offline audit file.**

   Interpret references to the "current audit file" as references to an offline audit file.

View Audit History

This section describes how you can view (on your workstation screen) the audit history for an offline audit file.

Prerequisites

Checklist

❑ See the "General Prerequisites" on page 29 and "Offline Report Prerequisites" on page 252.

Procedure

Procedure

1. **Choose "View audit history" from the "Reports from old offline files" menu (2602).**

   AUDITCON displays menu 2570.

2. **Follow the procedures in "View Audit History" on page 246 to view the audit history for an offline audit file.**

   Interpret references to the "current audit file" as references to an offline audit file.

Database Report Audit History

This section describes how you can generate a report of the audit history information in an offline audit file in a form suitable for loading into a database.

Prerequisites

Checklist

❑ See the "General Prerequisites" on page 29 and "Offline Report Prerequisites" on page 252.

Procedure

Procedure

1. **Choose “Database report audit history” from the “Reports from old offline files” menu (2602).**

   AUDITCON displays menu 2810.

2. **Follow the procedures in “Database Report Audit History” on page 248 to generate a text audit history report for an offline audit file.**

   Interpret references to the “current audit file” as references to an offline audit file.

External Audit Trail Maintenance

This section describes how you can use AUDITCON to copy, delete, and display the server’s old audit files. These mechanisms work only for old audit files, that is, the files maintained online by the server. You cannot perform these operations on offline audit data files. The only operation you can perform on the server’s current audit file is to reset the file, which causes the server to roll over to a new current audit file.

Audit File Maintenance Prerequisites

Checklist

❑ See the “General Prerequisites” on page 29.

Procedure

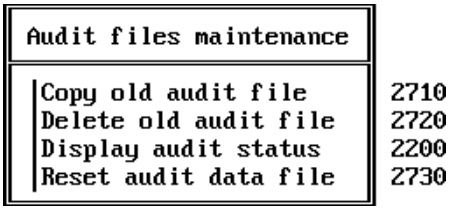
Procedure

1. **Choose “Audit files maintenance” from the “Available audit options” menu (2101).**

2. **Press** Enter**.**

   AUDITCON displays menu 2700, which lists more maintenance options. These options are described in the following sections.

Figure 6-17
Menu 2700: Audit Files Maintenance



Copy Old Audit File

This section describes how to copy old online audit files to removable media (for example, diskettes or magnetic tapes), workstation directories, or network drives. The primary reason for copying an audit file is to save the contents of the file before you delete it from the server. (see “Delete Old Audit File” on page 259). You might also want to copy an old audit file to removable media to save it for evidence or to keep it for long-term storage.

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.
- ❑ To copy an online audit file, you must have the Read right to the Audit File object Audit Contents property.
- ❑ You must have sufficient rights on your workstation or network drive to copy the audit file to that directory. For network drives, you must have at least the Create right. See your client documentation for more information on rights required to create a file on a hard drive or diskette.

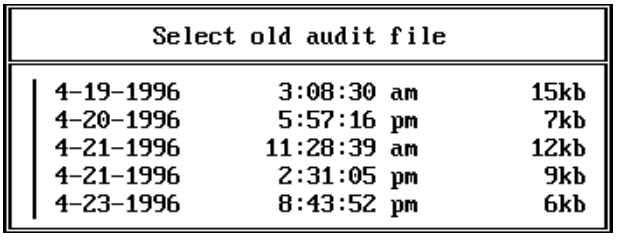
Procedure

Procedure

1. **Choose “Copy old audit file” from the “Audit files maintenance” menu (2700).**

   AUDITCON displays menu 2710, which lists up to 15 old audit files that are maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 6-18
Menu 2710: Select Old Audit File



2. **Move the cursor to choose the desired audit file and press** Enter**.**

   AUDITCON then prompt you for the name of the offline audit file.

   There is no mechanism for copying the contents of the current audit file. If you want to copy this data, you must first reset the audit data file (see "Reset Audit Data File" on page 260).

   You can only copy one file at a time. If you want to copy multiple audit files, perform the steps in this section once for each file.

3. **Enter the filename of the destination audit file and press** Enter**.**

   The pathname must be a DOS pathname on your local workstation, for example, "A:\AUDIT301.DAT", "C:\AUDIT\FILE1.DAT", or "F:\AUDITOR\VOL1\A950224.DAT." If you do not specify a drive letter and directory, AUDITCON will leave the audit file in your current directory. The default pathname is "AUDITOLD.DAT" on your local drive.

   AUDITCON displays a "Please wait" message while it copies the audit file from the server to your offline destination file. When it has copied the file, AUDITCON returns to menu 2700.

4. **If you copy audit files from the server onto your local workstation's file system, you must ensure that the audit data is properly protected by your workstation.**

5. **If you copy the audit file onto removable media (for example, a diskette or tape cartridge), attach a diskette or tape label that shows the server name, volume name, your name, the date, time, and size of the audit file, along with any other specific comments that you feel are important. Finally, you must ensure that the media is physically protected.**

   The purpose of this information is to ensure that you can load the medium in the future and generate meaningful audit reports from it.

   One strategy that is commonly used is to set the maximum audit file size so that one audit file will fit on a 1.44 MB diskette. See "Audit Options Configuration" on page 70 for information on setting the audit file size.

If you have a high volume of audit data, you will probably want to archive your audit files onto magnetic tape, for example, tape cartridges. AUDITCON does not provide a means for copying audit files directly to magnetic tape. If you want to use magnetic tape for long-term storage, you must first copy those files onto your file system, then use a backup program to copy the files to magnetic tape.

The frequency at which you copy the server's audit files to offline storage depends on how fast your server fills up audit files. If your server rolls over audit files on a periodic basis (as opposed to filling up the audit file), then you can set the number of audit files to 10 or 15, and copy/remove online audit files once per week without expecting to overflow the number of audit files.

Delete Old Audit File

This section describes how to delete an old audit file from the server after you've copied the file to offline storage or decided that you do not need to save the file.

Prerequisites

Checklist

- ❑ See the "General Prerequisites" on page 29.
- ❑ To delete an online audit file, you must have the Write right to the Audit File object Audit Policy property.

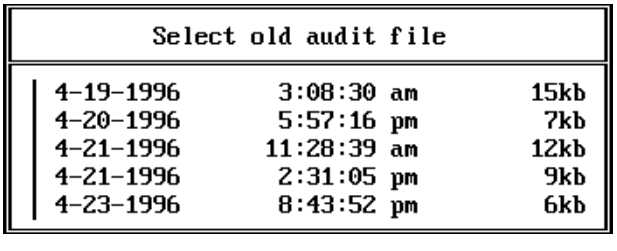
Procedure

Procedure

1. **Choose "Delete old audit file" from the "Audit files maintenance" menu (2700).**

   AUDITCON displays menu 2720, which lists up to 15 old audit files that are maintained online by the server. The old audit files are sorted by date and time (oldest first). The dates and times displayed show when the audit file was created (that is, when it started accumulating audit events).

Figure 6-19
Menu 2720: Select Old Audit File



Note

There is no mechanism for deleting the current audit file. If you want to delete the data in the current audit file, you must first reset the audit data file (“Reset Audit Data File” in this chapter).

You can only delete one file at a time. If you want to delete multiple audit files, perform the steps in this section once for each file.

2. **Move the cursor to choose the desired audit file, then press** Enter**.**

   AUDITCON asks you to confirm that you want to delete the audit file.

Warning

After you delete an online audit file, there is no way to recover the contents of the file. Do not delete the file unless you are absolutely certain that you will not require the data in the audit file. If there is any doubt, copy the audit file to offline storage before you delete the file.

Reset Audit Data File

This section describes how to reset the current audit file. Reset is a manual means of causing the current audit file to “roll over,” that is, to cause the current audit file to become an old audit file and to establish a new current audit file.

Manual reset might be necessary, for example, if the server stops processing external audit requests because the external audit trail is in an overflow state. See “Trail Problems” on page 261 for information on recovering from external audit trail overflow.

Prerequisites

Checklist

- ❑ See the “General Prerequisites” on page 29.
- ❑ To reset the current audit file, you must have the Write right to the Audit File object Audit Policy property.

Procedure

Procedure

1. **Choose “Reset audit data file” from the “Audit files maintenance” menu (2700).**

   AUDITCON requests confirmation that you want to perform the reset.

If you perform the reset the current audit file will become an old audit file and a new current audit file will be created.

2. **Choose "Yes" and press** Enter **to reset the current external audit file.**

Trail Problems

This section describes solutions to potential external audit trail problems. These include audit trail overflow and recovery from catastrophic failures.

Audit Trail Overflow

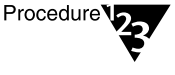
"Preventing Loss of Audit Data" on page 23 describes the potential for audit loss if the configured number of audit files are filled or disk space fills up and the audit trail is improperly configured.

"Audit Options Configuration" on page 235 describes the three overflow configuration options for external audit trails:

- Archive audit file
- Disable record submission
- Disable event recording

The only option that prevents the loss of audit events (from audit overflow situations) is to disable record submission. With this setting, the server stops accepting externally generated events either when the current audit file has reached the "Audit file maximum size" or the server cannot write the current audit file (for example, it is out of disk space).

Procedure



Use the following steps to deal with audit trail overflow.

1. **Log in as an auditor with sufficient rights to the external audit trail's Audit File object.**

2. **If you want to save the oldest audit file, and you haven't already backed it up, copy the oldest old audit file to offline storage (for example, a file in the server or workstation or removable media).**

3. **Reset the current external audit file, as described in "Reset Audit Data File" on page 260 in this chapter.**

   This archives the current audit file (to an old audit file), deleting the oldest old audit file, and creates a new audit file.

4. **If you want to save any audit files that you haven't already saved (including the newest of the old audit files), copy those audit files to offline storage.**

The following pointers help prevent external audit trail overflow:

1. Review the status and size of the audit file frequently.
2. Manually reset the audit file before it overflows, if necessary.
3. Enable "Automatic audit file archiving" as described in "Audit Options Configuration" on page 235. Set the "Audit file maximum size" large enough and the "Days between audit archives" low enough that the audit file will not overflow.
4. Don't over audit.

If the external audit trail is full, the auditor's actions (for example, deleting data files, resetting the audit file) might not be audited. In this case, you must keep a manual log of your actions for use when generating a complete history of actions performed on the server. You will be informed via a message from the server to your workstation when this occurs.

When the audit trail is reaches its configured threshold, you will receive the following notification on your workstation screen:

```
The audit overflow file for external auditing Audit
File objectname is almost full.  Auditors must begin
manual auditing now!
```

When the audit trail is completely full, you will receive the following notification on your workstation screen:

```
The audit overflow file for external auditing Audit
File objectname is full.
```

To avoid missing this message, you must not issue the SEND /A=N or SEND /A=P commands (or if using Windows and the NetWare User Tools, do not disable network warnings), as they would cause these messages to be suppressed.

Catastrophic Failure Recovery

This section describes what to do if a catastrophic failure destroys the volume containing the external audit data is destroyed. One such catastrophic failure would be hard disk failure. You will need to return the audit data to the state it was in before the failure.

This section also explains how to handle planned upgrades, such as moving a volume moved from a small disk to a larger disk.

There are several potential losses not addressed here:

- Loss of offline audit data. Your offline audit data (whether it's stored in server or workstation file systems or on removable media) should be backed up frequently enough that its loss would not be catastrophic.

- Loss of some, but not all copies of the Audit File object describing the external audit trail due to failure of one or more servers holding an NDS partition. In this case, NDS will automatically use whatever copies are available. If a server configured for the partition is brought back online, then it will automatically be updated with the Audit File object information.

There are two major catastrophic failures possible for external audit.

- Loss of all copies of the Audit File object describing the external audit trail. If all copies of the Audit File object are lost (for example, because there only was one copy, and the server it was on suffered a disk failure), then you might be able to recover the Audit File object from a backup of your Directory tree (presuming you have backed up your Directory tree). If so, then you can regain access to the existing online audit data. If not, then no access is possible to the online audit data. You must re-create the external audit trail using the procedures in "Create External Audit Trail" on page 228.

- Loss of the volume containing the external audit data (for example, because of a disk failure). Because external audit files are

stored in an inaccessible directory which cannot be backed up, loss of the volume means that the online audit files (both the current audit file and any old audit files) are lost. You should use AUDITCON to perform regular backups of audit data to avoid loss of online audit data.

In addition to loss of the online audit data, loss of the volume means that the server will no longer have the information it needs to accept additional audit records. If this occurs, you should enable auditing using the procedures in "Create External Audit Trail" on page 228.

Upgrade of a volume (for example, replacing it with a larger disk) is equivalent to recovering from a catastrophic disk failure. To do an upgrade, you must first back up the old volume, and then restore it on the new disk. This loses all audit data. Therefore, before performing a volume upgrade, you should also back up all external audit data. After the new disk is installed, you should enable the external audit trail using the procedures in "Create External Audit Trail" on page 228.

Immediacy of Changes

When you modify the external audit trail configuration (for example, to change the maximum size of the audit file), the change is made both to the Audit Policy property of the Audit File object and to the header of the current audit file. Both changes will usually occur immediately.

However, the effect of the change might not be immediate if the server holding the audit data is unavailable to receive the configuration change (for example, because it is down or the network has been split), even though the Audit File object can be modified. In this case, the delay depends on how long it takes before the two servers can synchronize their NDS replicas.

See "Viewing and Managing NDS Synchronization Status (Console)" in *NetWare Enhanced Security Administration* for information on how to determine when synchronization occurs.

In addition, changes to the ACL of the Audit File object that represents the external audit trail do not affect any connections that have already been established. That is, if a workstation has already started uploading audit data to a server, changing the ACL will not affect that workstation's ability to perform uploads.

To force a workstation to stop uploading data immediately, you should break that workstation's connection to the server using the console MONITOR utility or the CLEAR STATION console command.

Similarly, if an auditor is performing audit trail management functions, changing the ACL will not affect the auditor's capabilities (either to increase or decrease them). An auditor's rights are recalculated every time he or she restarts AUDITCON and establishes access to an audit trail. To stop the auditor's actions immediately, you should break the auditor's connection to the server using the console MONITOR utility or the CLEAR STATION console command.

appendix **A**

Audit File Formats

This appendix defines the audit file formats for volumes, containers, and external audit trails. For definitions of the types of audit trails, see Table 1-1.

Volume Audit Format

Each volume audit file is a file in an inaccessible directory in the volume. That is, the audit files for volume SYS: are maintained in an inaccessible directory on volume SYS: , and the audit files for volume ALPHA: are kept in an inaccessible directory on volume ALPHA:.

The inaccessible directories are protected, hidden directories that network clients cannot directly read by issuing file and directory NCP™ messages. The names of the audit files are derived by the server from the name of the Audit File object when each file is created; however, these filenames are not meaningful outside the server's auditing software.

Each volume audit file consists of a header (that includes data such as creation time) and a sequence of audit event records. That is, the server appends discrete volume audit records to the associated current audit file.

Audit files are not necessarily a fixed size. The server writes an audit record, then checks to see whether the audit file has exceeded the desired size. If so, the server executes a background thread to perform the file rollover; however, during this time, the server might add even more events before the file is rolled over.

Records within a volume audit file are sequenced in order of increasing time, using the server's local time. Note that time discontinuities in the audit trail can occur if the server's time is modified.

Records are stored in the audit file in a "null-compressed" format (0xE0 = 1 null byte, 0xE1 = 2 null bytes, ..., 0xEE = 15 null bytes, 0xEF = next byte actual). After encoding all natural nulls in the audit record, the server then uses a null character (0x00) as a record separator.

Each audit file is self-contained; that is, you don't have to read previous audit files to establish the context for the current file. For example, if a user is logged in when the audit file rolls over, the server writes a pseudo-login event for that user. If a file is open when the audit file rolls over, the new audit file contains a pseudo-open event.

The following sections describe the format of volume audit files internally, within the server, and as displayed by AUDITCON.

Volume Audit File Header

Each volume audit file contains an audit file header that defines the audit status and configuration data for the audit file. Table A-1 defines the format of the volume audit file header. The data types "BYTE", "WORD", and "LONG" refer to 8-, 16-, and 32-bit integers, respectively. The "BYTE" data type is also used for character strings.

Table A-1
Volume Audit File Header

Type	Identifier	Description
WORD	fileVersionDate	Current version of the audit file.
BYTE	auditFlags	Bit map, including concurrent auditor access, dual-level passwords, broadcast warnings to all users.
BYTE	errMsgDelayMinutes	Number of minutes to delay between error messages.
BYTE	encryptPassword[16]	Encrypted level 1 password hash value (not used in evaluated configuration)
LONG	volumeAuditFileMaxSize	Nominal audit file maximum size.
LONG	volumeAuditFileSizeThreshold	Nominal audit file size threshold.
LONG	auditRecordCount	Number of user audit records in file.
LONG	historyRecordCount	Number of auditor event records in file.

Table A-1 *continued*
Volume Audit File Header

Type	Identifier	Description
BYTE	encryptPassword2[16]	Encrypted level 2 password hash value (not used in evaluated configuration).
LONG	spare[2]	Unused.
LONG	overflowFileSize	Size of overflow file.
bit map	volumeAuditEventBitMap	Unused; see newBitMap definition.
LONG	aFileCreationDateTime	Audit file creation time.
BYTE	randomData[8]	Unused.
WORD	auditFlags2	Unused.
WORD	fileVersionDate2	Unused.
BYTE	fileArchiveDays	Days between audit archive.
BYTE	fileArchiveHour	Hour of day to archive.
BYTE	numOldAuditFilesToKeep	Number of old audit files to keep (1-15).
BYTE	spareByte	Unused.
LONG	hdrChecksum	Checksum of header.
LONG	spareLongs[2]	Unused.
BYTE	newBitMap[64]	Bitmap of audit events selected for this volume.
BYTE	spareBytes[64]	Unused.
BYTE	auditObjectDN[514]	Distinguished (complete) name of Audit File object associated with the volume.
BYTE	spareBytes2[122]	Unused.
LONG	wrappedDataKeyLength	Unused.
LONG	wrappedDataKey[1152]	Unused.

For more information, refer to the corresponding status information in “Displaying Volume Audit Status” on page 43 and volume configuration information in the “Audit Options Configuration” on page 70.

Volume Audit Record Format

This section defines the binary format of each audit record in the volume audit trail. Each audit record has a fixed record header and, potentially, additional event-specific data.

The volume audit record header (audit_rec_hdr) is a fixed structure that contains data for each audit event in the audit file. Table A-2 shows the fields in each volume audit record header.

Table A-2
Volume Audit Record Header

Type	Element Name	Description
WORD	eventTypeID	Volume audit event type, from Table A-3 or Table A-4
WORD	chkWord	Checksum, used for internal integrity checks.
LONG	connectionID	Server’s internal connection table entry. This value is used to associate an event with the user that performed that event.
LONG	processUniqueID	Client process ID. This value can be used to trace client events (for example, file opens) to a specific process on that client.
LONG	successFailureStatusCode	Completion status: 0=successful, non-zero=failure.
WORD	dosDate	DOS-format date of event.
WORD	dosTime	DOS-format time of event.

Table A-3 defines each volume audit file record name and number, describes the type of event (accounting, extended attribute, file, message, QMS, server, user), when it is generated, and the format of any additional event-specific data in the audit record. The data types "BYTE", "WORD", and "LONG" refer to 8-, 16-, and 32-bit integers,

respectively. The "BYTE" data type is also used for character strings. The complete name of each event in Table A-3 starts with "A_EVENT_"; that prefix is omitted to save room.

Events 29 through 41, 228 through 235, and 261 are queue management events. Queue management events are always recorded in the audit trail of volume SYS:, and therefore will not appear in the audit trails of any other volumes.

Table A-3
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
7	CHANGE_DATE_TIME Server event, audits time/date change.	LONG; DosDateTime; Old DOS format Date/ Time
10	CLOSE_FILE File event, audits user file close.	LONG; Handle; File handle LONG; Modified; Set if file was modified
12	CREATE_FILE File event, audits user file creation.	LONG; Handle; DOS file handle LONG; Rights; Requested open rights LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
14	DELETE_FILE File event, audits user file deletion.	LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
17	DISABLE_ACCOUNT User event, audits disabling a user account.	BYTE; FileName[ ]; Length-preceded Bindery username
18	DOWN_SERVER Server event, audits server shutdown.	(None)

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
19	GRANT_TRUSTEE	LONG; TrusteeID; User ID of trustee
	User event, audits assignment of trustee rights to a user.	LONG; Rights; Assigned trustee rights
		LONG; NameSpace; DOS name space
		BYTE; TrusteeName[ ]; Length-preceded username
		BYTE; FileName[ ]; Length-preceded directory pathname
21	LOGIN_USER	LONG; UserID; User entry ID on server
	User event, audits user login or background authentication to a server.	BYTE; NetworkAddrType; IPX=1
		BYTE; NetworkAddrLen; Length (IPX uses 10)
		BYTE; NetworkAddress; IPX network address
		BYTE; Name[ ]; Length-preceded username
23	LOGOUT_USER	LONG; UserID; User entry ID on server
	User event, user logout from a server.	BYTE; Name[ ]; Length-preceded username

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
25	MODIFY_ENTRY File event, audits user modification of a directory entry.	LONG; ModifyBits; Bitmap indicating modifications made LONG; NameSpace; DOS name space BYTE; ModifyStruct[ ]; Array of modifications BYTE; FileName[ ]; Length-preceded pathname BYTE; OldDosName[ ]; Length-preceded old filename (optional) BYTE; NewOwner[ ]; Length-preceded owner name (optional) BYTE; LastArchivedBy; Length-preceded username (optional) BYTE; LastModifiedBy; Length-preceded username (optional)
27	OPEN_FILE File event, audits user file open.	LONG; Handle; DOS file handle LONG; Rights; Requested open rights LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
29	Q_ATTACH_SERVER QMS event, audits assignment of an object to a queue's list of queue servers.	BYTE; Qname[ ]; Length-preceded queue name BYTE; Servername[ ]; Length-preceded server name
29	Q_CREATE QMS event, audits creation of a queue object and its associated queue directory.	LONG; QType; Queue type BYTE; FileName[ ]; Length-preceded queue name

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
30	Q_CREATE_JOB QMS event, audits creation of a queue job.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
31	Q_DESTROY QMS event, audits deletion of a queue object, queue directory, and associated job files.	LONG; QType; Queue type BYTE; QName[ ]; Length-preceded queue directory name
32	Q_DETACH_SERVER QMS event, audits removal of an object from a queue's list of queue servers.	BYTE; Qname[ ]; Length-preceded queue name BYTE; Servername[ ]; Length-preceded server name
33	Q_EDIT_JOB QMS event, edit parameters associated with queue job.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDesc[ ]; Null-terminated previous job description BYTE; NewJobDesc[ ]; Null-terminated new job description
34	Q_JOB_FINISH QMS event, audits completion of queue job by a queue server.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
35	Q_JOB_SERVICE QMS event, audits selection of next available queue job by queue server.	LONG; TType; Queue target type BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
36	Q_JOB_SERVICE_ABORT QMS event, audits abnormal termination of queue job by queue server.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
37	Q_REMOVE_JOB QMS event, audits removal of an entry from a queue.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
38	Q_SET_JOB_PRIORITY QMS event, audits change of queue job priority.	LONG; Priority; Queue job priority BYTE; QName[ ]; Length-preceded queue name BYTE; JobDesc[ ]; Null-terminated job description
39	Q_SET_STATUS QMS event, audits a change of queue status by queue operator.	LONG; Status; Queue status bitmap BYTE; QName[ ]; Length-preceded queue name
40	Q_START_JOB QMS event, audits making an entry ready for service.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
41	Q_SWAP_RIGHTS QMS event, records the change of rights (by a queue server) to match the rights of the user that placed the job in the queue.	BYTE; QName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Null-terminated job description
42	READ_FILE File event, audits user read of open file.	LONG; Handle; Open file handle LONG; ByteCount; # of bytes actually read LONG; Offset; File offset

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
43	REMOVE_TRUSTEE User event, audits removal of trustee from file or directory.	LONG; TrusteeID; User ID of trustee LONG; Rights; Trustee rights LONG; NameSpace; DOS name space BYTE; TrusteeName[ ]; Length-preceded username BYTE; FileName[ ]; Length-preceded directory pathname
44	RENAME_MOVE_FILE File event, audits rename or move of file.	LONG; NameSpace; DOS name space BYTE; FileName1[ ]; Length-preceded name, before operation BYTE; FileName2[ ]; Length-preceded name, after operation
46	SALVAGE_FILE File event, audits salvage of deleted file space.	LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
49	TERMINATE_CONNECTION User event, audits termination of user connection.	LONG; ConnectionNbr; Number of the connection that was terminated
50	UP_SERVER Server event, audits start of server. (Note: this event cannot be preselected by AUDITCON).	(None)
53	USER_SPACE_RESTRICTIONS User event, record change of a user's volume space restriction.	LONG; SpaceValue; User space restriction (blocks per volume) BYTE; TrusteeName; Length-preceded trustee name

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
55	VOLUME_MOUNT Server event, audits mount of disk volume.	(None)
56	VOLUME_DISMOUNT Server event, audits dismount of disk volume.	(None)
57	WRITE_FILE File event, audits user write to open file.	LONG; Handle; Open file handle LONG; ByteCount; # of bytes actually written LONG; Offset; File offset
75	CREATE_DIRECTORY File event, records user creation of directory.	LONG; Handle; DOS file handle LONG; Rights; Requested open rights LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
76	DELETE_DIRECTORY File event, records user deletion of directory.	LONG; NameSpace; DOS name space BYTE; FileName[ ]; Length-preceded pathname
200	GET_CURRENT_ACCOUNT_-STATUS Accounting event, records querying the current account status	BYTE; ClientName[ ]; User whose status is requested
201	SUBMIT_ACCOUNT_CHARGE Accounting event, records submitting an accounting charge.	BYTE; ClientName[ ]; User whose account is being charged
202	SUBMIT_ACCOUNT_HOLD Accounting event, records submitting an accounting hold	BYTE; ClientName[ ]; User whose account is being held

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
203	SUBMIT_ACCOUNT_NOTE Accounting event, records submitting an accounting note	BYTE; ClientName[ ]; User whose account is being noted
204	DISABLE_BROADCASTS Message event, records refusal of future messages.	(None)
205	GET_BROADCAST_MESSAGE Message event, records retrieving a message sent to the connection.	(None)
206	ENABLE_BROADCASTS Message event, records acceptance of future messages.	(None)
207	BROADCAST_TO_CONSOLE Message event, records sending a message to the server console.	(None)
208	SEND_BROADCAST_MESSAGE Message event, records sending a message to a connection. If message was sent to more than one recipient, a separate audit record is recorded for each recipient.	BYTE; ClientName[ ]; User to whom message was sent
209	WRITE_EATTRIB Extended attribute event, records writing the extended attributes of a file.	BYTE; PathName[ ]; Length-preceded pathname

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
210	READ_EATTRIB Extended attribute event, records reading the extended attribute of a file.	BYTE; PathName[ ]; Length-preceded pathname
211	ENUM_EATTRIB Extended attribute event, records enumeration of extended attributes.	BYTE; PathName[ ]; Length-preceded pathname
212	SEE_FSO File event, records examining an FSO for computing rights or handle.	BYTE; PathName[ ]; Length-preceded pathname
213	GET_FSO_RIGHTS File event, records computing a user's rights to a file system object.	BYTE; PathName[ ]; Length-preceded pathname
214	PURGE_FILE File event, records purging a file.	LONG; NameSpace; DOS name space BYTE; PrimEntryName[ ]; Primary filename
215	SCAN_DELETED File event, records scanning the list of deleted files.	BYTE; PathName[ ]; Length-preceded path name scanned
216	DUPLICATE_EATTRIB Extended attribute event, records duplication of extended attribute.	BYTE; DestPathName[ ]; Length-preceded pathname of destination BYTE; SrcPathName[ ]; Length-preceded pathname of source file
217	ALLOC_SHORT_DIRECTORY_HANDLE File event, records allocation of directory handle	LONG; DirectoryHandle; Existing directory handle BYTE; PathName[ ]; Length-preceded pathname for new handle

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
218	SET_HANDLE File event, records computation of directory handle.	BYTE; PathName[ ]; Length-preceded pathname for new handle
219	SEARCH File event, records searching for FSOs.	BYTE; PathName[ ]; Length-preceded pathname being searched for
220	GEN_DIR_BASE_AND_VOL File event, records accessing an FSO	BYTE; PathName[ ]; Length-preceded pathname
221	OBTAIN_FSO_INFO File event, records obtaining FSO information.	BYTE; PathName[ ]; Length-preceded pathname
222	GET_REF_COUNT File event, records retrieving reference count.	BYTE; PathName[ ]; Length-preceded pathname
223	MODIFY_ENTRY_NO_SEARCH File event, records modifying an FSO's information.	BYTE; PathName[ ]; Length-preceded pathname
224	SCAN_TRUSTEES File event, records scanning the list of FSO trustees.	BYTE; PathName[ ]; Length-preceded pathname
225	GET_OBJ_EFFECTIVE_RIGHTS File event, records computation of effective rights to a given file for a given NDS object.	BYTE; PathName[ ]; Length-preceded pathname BYTE; ObjectName[ ]; NDS object for which rights are questioned
226	PARSE_TREE File event, records scanning the FSO tree.	BYTE; PathName[ ]; Length-preceded pathname

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
227	SET_SPOOL_FILE_FLAGS Queue event, records setting the spool file flags.	LONG; PrintFlags; New flags for the spool file
228	RESTORE_Q_SERVER_RIGHTS Queue event, records restoring a queue server's previous rights & identity.	(None)
229	Q_JOB_SIZE Queue event, records retrieving a queued job's size.	BYTE; QueueName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Length-preceded job description
230	Q_JOB_LIST Queue event, records retrieving the list of jobs in a queue.	BYTE; QueueName[ ]; Length-preceded queue name
231	Q_JOB_FROM_FORM_LIST Queue event, records retrieving the list of jobs waiting for a form.	BYTE; QueueName[ ]; Length-preceded queue name
232	READ_Q_JOB_ENTRY Queue event, records reading information about a queued job.	BYTE; QueueName[ ]; Length-preceded queue name BYTE; JobDescription[ ]; Length-preceded job description
233	MOVE_Q_JOB Queue event, records moving a job from one queue to another.	BYTE; SrcQueueName[ ]; Length-preceded source queue name BYTE; DestQueueName[ ]; Length-preceded destination queue name BYTE; JobDescription[ ]; Length-preceded job description

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
234	READ_Q_STATUS Queue event, records querying the status of a queue.	BYTE; QueueName[ ]; Length-preceded queue name
235	READ_Q_SERVER_STATUS Queue event, records querying the status of a queue server.	BYTE; QueueName[ ]; Length-preceded queue name BYTE; ServerName[ ]; Length-preceded server name
236	EXTENDED_SEARCH File event, records use of extended file searching.	BYTE; PathName[ ]; Length-preceded pathname
237	GET_DIR_ENTRY File event, records getting a directory entry.	BYTE; PathName[ ]; Length-preceded pathname
238	SCAN_VOL_USER_RESTR File event, records getting the user disk space restrictions for a volume.	(None)
239	VERIFY_SERIAL Server event, records verification of the server serial number.	(None)
240	GET_DISK_UTILIZATION File event, records retrieving the disk usage for a particular user on a volume.	BYTE; ClientName[ ]; Length-preceded username being queried BYTE; VolumeName[ ]; Length-preceded volume name being examined
241	LOG_FILE File event, records locking a file for exclusive use.	BYTE; FileName[ ]; Length-preceded pathname being locked

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
242	SET_COMP_FILE_SZ File event, records setting the file size of a compressed file	BYTE; FileName[ ]; Length-preceded pathname
243	DISABLE_LOGIN Server event, records console command to disallow logins.	(None)
244	ENABLE_LOGIN Server event, records console command to allow logins.	(None)
245	DISABLE_TTS Server event, records console command to disable transaction tracking.	(None)
246	ENABLE_TTS Server event, records console command to enable transaction tracking.	(None)
247	SEND_CONSOLE_BROADCAST Message event, records sending a message to the console	(None)
248	REMAINING_GET_OBJ_DISK_SPACE Server event, records getting the amount of disk space available	(None)
249	GET_CONN_TASKS Server event, records getting the list of tasks associated with a connection.	(None)

Table A-3 *continued*
Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
250	GET_CONN_OPEN_FILES Server event, records getting the list of files open by a connection.	(None)
251	GET_CONN_USING_FILE Server event, records getting the list of connections using a file.	(None)
252	GET_PHYS_REC_LOCKS_CONN Server event, records getting the list of physical record locks in use by a connection.	(None)
253	GET_PHYS_REC_LOCKS_FILE Server event, records getting the list of physical locks associated with a file.	(None)
254	GET_LOG_REC_BY_CONN Server event, records getting the list of logical record locks in use by a connection.	(None)
255	GET_LOG_REC_INFO Server event, records getting information about logical record locks.	(None)
256	GET_CONN_SEMS Server event, records getting the list of semaphores in use by a connection.	(None)
257	GET_SEM_INFO Server event, records getting information about a semaphore.	(None)

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
258	MAP_DIR_TO_PATH Server event, records mapping a directory number to a path name.	BYTE; PathName[ ]; Length-preceded pathname
259	CONVERT_PATH_TO_ENTRY Server event, records converting a path name to the entry number.	BYTE; PathName[ ]; Length-preceded path name
260	DESTROY_SERVICE_CONN Server event, records termination of a connection.	(None)
261	SET_Q_SERVER_STATUS Queue event, records setting a queue server status.	BYTE; QueueName[ ]; Length-preceded queue name BYTE; ServerName[ ]; Length-preceded server name
262	CONSOLE_COMMAND Server event, records a command at the server console.	BYTE; CommandLine[ ]; Command entered at console
263	REMOTE_ADD_NS Server event, records addition of a new name space from a remote workstation.	BYTE; NameSpaceName[ ]; Name of name space that is remotely added
264	REMOTE_DISMOUNT Server event, records volume dismount from a remote workstation.	BYTE; VolumeName[ ]; Name of volume that is remotely dismounted
265	REMOTE_EXE Server event, records execution of .NCF batch file from a remote workstation.	BYTE; PathName[ ]; Pathname of .NCF file that is remotely executed on server

Table A-3 *continued*

Volume Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
266	REMOTE_LOAD Server event, records loading of NLM from remote workstation.	BYTE; PathName[ ]; Pathname of NLM that is remotely loaded
267	REMOTE_MOUNT Server event, records mounting of volume from a remote workstation.	BYTE; VolumeName[ ]; Name of volume that is remotely mounted
268	REMOTE_SET Server event, records modification of a server SET parameter from a remote workstation.	BYTE; SetParmCommand[ ]; Command line, including new value, for change to server SET parameter
269	REMOTE_UNLOAD Server event, records unloading of NLM from a remote workstation.	BYTE; PathName[ ]; Pathname of NLM that is remotely unloaded.

Table A-4 defines the volume audit file event names, numbers, and event specific data for the audit history events. Audit events marked with an asterisk (*) will not occur in the evaluated configuration, because passwords are not used for access control. The complete name of each event in Table A-4 starts with "AUDITING_"; that prefix is omitted to save room.

Table A-4
Volume Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
58	ACTIVE_CONNECTION_RCD Records establishment of an active connection. This is the means used to associate a user's identity with subsequent operations on a connection. After an audit file is reset, active connections are written to new audit file.	LONG UserID; User entry ID on server BYTE NetworkAddrType IPX=1 BYTE NetworkAddrLen; Length (IPX uses 10) BYTE NetworkAddress; IPX network address BYTE Name[ ]; Length-preceded username
59 (*)	ADD_AUDITOR_ACCESS Records an auditor gaining access to audit trail by providing the password.	LONG UserID; User entry ID on server BYTE NetworkAddrType IPX=1 BYTE NetworkAddrLen; Length(IPX uses 10) BYTE NetworkAddr; IPX network address BYTE Name[ ]; Length-preceded username
60	ADD_AUDIT_PROPERTY Records setting the per-user audit flag.	BYTE Name[ ]; Length-preceded username that was marked
61 (*)	CHANGE_AUDIT_PASSWORD Records a change to level 1 password.	(None)
62	DELETE_AUDIT_PROPERTY Records clearing the per-user audit flag.	BYTE Name[ ]; Length-preceded username that was cleared

Table A-4 *continued*

Volume Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
63	DISABLE_VOLUME_AUDIT Records disabling of auditing on current volume.	(None)
64	OPEN_FILE_HANDLE_RCD Records file handle and name. After an audit file is reset, this event identifies file handles currently in use.	LONG FileHandle; Allocated file handle LONG Unused; For future expansion LONG NamespaceID; Name space, DOS=1 BYTE Name[ ]; Length-preceded filename that was opened
65	ENABLE_VOLUME_AUDITING Records an auditor's enabling volume auditing.	(None)
66	REMOVE_AUDITOR_ACCESS Records an auditor relinquishing access to the audit trail.	(None)
67	RESET_AUDIT_FILE Records an auditor rolling over to a new audit file. This is the last record in the old audit file.	(None)
68	RESET_AUDIT_FILE2 Records an auditor rolling over to a new audit file. This is the first record in the new audit file.	(None)
70	WRITE_AUDIT_BIT_MAP Records change to audit file bitmap (that is, change to set of preselected volume audit events).	(None)

Table A-4 *continued*

Volume Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
71	WRITE_AUDIT_CONFIG_HDR Records write of configuration data to audit file header.	(None)
72	NLM_ADD_RECORD1 Records a history event generated by an NLM.	LONG RecordTypeID; As defined by NLM LONG DataLen; Length of NLM provided data BYTE UserName[ ]; Length-preceded username provided by NLM BYTE Data[ ]; NLM provided data
73	ADD_NLM_ID_RECORD2 Record the identity of an NLM that generates audit records.	LONG NLMid; Novell-defined NLM ID BYTE NetworkAddrType IPX=1 BYTE NetworkAddrLen; Length (IPX uses 10) BYTE NetworkAddr; IPX network address
74 (*)	CHANGE_AUDIT_PASSWORD2 Generated when level 2 password is changed.	(None)
77 (*)	INTRUDER_DETECT Generated when a user fails log in to an audit file because the incorrect password was provided.	LONG UserID; User entry ID on server BYTE NetworkAddrType IPX=1 BYTE NetworkAddrLen; Length (IPX uses 10) BYTE NetworkAddr; IPX network address BYTE Name[ ]; Length-preceded username
80	VOLUME_NAME_RCD_2 Generated at beginning of volume audit file.	BYTE Name[ ]; Length-preceded NDS distinguished name of volume BYTE Null[ ]; Unused string
81	DELETE_OLD_AUDIT_FILE Records deletion of an old audit file.	(None)

Table A-4 *continued*
Volume Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
82	QUERY_AUDIT_STATUS Records gaining access to the audit file.	(None)

Events 58 (AUDITING_ACTIVE_CONNECTION_RCD), 64 (AUDITING_OPEN_FILE_HANDLE_RCD), and 80 (AUDITING_VOLUME_NAME_RCD2) are pseudo-events (that is, they do not represent actual events).

Pseudo-events are used so that each audit data file can be self-contained. For example, if a user logs in, event 21 (A_EVENT_LOGIN_USER) is generated (as shown in Table A-3). If a subsequent audit reset occurs, the pseudo-event 58 would be generated for each logged-in user, so the new audit data file would have a record of all logged in users (thus making subsequent references in the audit file to connection numbers meaningful).

Similarly, if a user opens a file, event 27 (A_EVENT_OPEN_FILE) is generated (as shown in Table A-3). If a subsequent audit reset occurs, the pseudo event 64 would be generated for each file open by each user, so the new audit data file would have a record of all open files (thus making subsequent references in the audit file to file handles meaningful).

Event 80 is always the first audit event in each audit file, recording the volume which caused generation of the audit file.

Textual Audit Format (AUDITCON)

There is a one-to-one correspondence between the binary audit record format and the textual representation of the event. Note, however, that the output of a textual audit event depends upon the context of the event, for example, the association of a file handle with a filename. Refer to “View Audit File” on page 109 and “View Old Audit File” on page 112 for examples of the AUDITCON report format.

Container Audit Format

Container audit files are treated as an extension of the container itself. Consequently, container audit files are replicated to the same servers on which the container itself is replicated. These replicas are maintained in an inaccessible directory in volume SYS: of the servers where the container is replicated.

The inaccessible directory is a protected directory that network clients cannot directly read by issuing file and directory NCP messages. The names of the audit files are derived by the server from the name of the Audit File object when each file is created; however, these filenames are not meaningful outside the server's auditing software.

Each container audit file consists of a header (such as creation time) and a sequence of audit event records. Audit records are usually, but not necessarily, sequenced in order of increasing time.

Because of the way DS.NLM synchronizes NDS™ audit data, events might be recorded in an arbitrary order. The ordering of events in one replica of an audit file might not be the same as the ordering of events in a different replica. However, while replicated audit files are not necessarily identical, an audited event will nearly always show up as an audit record for each replica.

Container audit files are not necessarily a fixed size. The server writes an audit record, then checks to see whether the audit file has exceeded the desired size. If so, the server executes a background thread to perform the file rollover; however, during this time, the server might add even more events before the file is rolled over. Because of the synchronization of audited events to replicas on different servers, individual replicas of audit files are not necessarily the same size.

Records are stored in the audit file in a "null-compressed" format (0xE0 = 1 null byte, 0xE1 = 2 null bytes, ..., 0xEE = 15 null bytes, 0xEF = next byte actual). After encoding all natural nulls in the audit record, the server then uses a null character (0x00) as a record separator.

The following sections describe the internal format of audit files within the server ("internal format") and the AUDITCON display format for each audit trail.

Container Audit File Header

Each container audit file contains an audit file header that defines the audit status and configuration data for the audit file. Table A-5 defines the format of the container audit file header. The data types "uint8", "uint16", and "uint32" refer to 8-, 16-, and 32-bit integers, respectively.

Table A-5
Container Audit File Header

Type	Identifier	Description
uint16	fileVersionDate	Current version of the audit file
uint8	auditFlags	Bitmap, including concurrent auditor access, dual-level passwords, broadcast warnings, and others.
uint8	errMsgDelayMinutes	Number of minutes to delay between error messages.
uint32	containerID	NDS directory ID for container.
uint32	overflowFileSize	Size of overflow file.
uint32	creationTS[2]	Timestamp for creation of the container.
uint32	bitMap	Unused; see newBitMap.
uint32	auditFileMaxSize	Nominal audit file maximum size.
uint32	auditFileSizeThreshold	Nominal audit file size threshold.
uint32	auditRecordCount	Number of user audit records in file.
uint16	replicaNumber	NDS replica number.
uint8	enabledFlag	Indicates whether auditing is enabled for the container.
uint8	fileArchiveDays	Days between audit archive.
uint8	fileArchiveHour	Hour of day to archive.
uint8	numOldAuditFilesToKeep	Number of old audit files to keep (1-15).
uint16	numberReplicaEntries	Number of replicas in the ring for this container.

Table A-5 *continued*

Container Audit File Header

Type	Identifier	Description
uint32	aFileCreationDateTime	Time & date this audit file was created.
uint8	randomData[8]	Unused.
uint32	partitionID	Directory partition number.
uint32	hdrChecksum	Checksum of header.
uint32	spareLongs[4]	Unused.
uint32	auditDisabledCounter	Number of times the container audit trail has been disabled.
uint32	auditEnabledCounter	Number of times the container audit trail has been enabled.
uint8	encryptPassword[16]	Encrypted level 1 password hash value (not used in evaluated configuration).
uint8	encryptPassword2[16]	Encrypted level 2 password hash value (not used in evaluated configuration)
uint32	hdrModifiedCounter	Number of times the header has been modified.
uint32	fileResetCounter	Number of times the container audit trail has been reset (archived).
uint8	newBitMap[64]	Bitmap of audit events being recorded.
uint8	spareBytes[64]	Unused.
uint8	auditObjectDN[514]	Distinguished (complete) name of Audit File object associated with the volume.
uint8	spareBytes2[122]	Unused.
uint32	wrappedDataKeyLength	Unused.
uint32	wrappedDataKey[1152]	Unused.

For more information, refer to the corresponding status information in “Displaying Container Audit Status” on page 151 and container

configuration information in “Audit Options Configuration” on page 164.

Container Audit Record Format

This section defines the binary format of each audit record in the container audit trail. Each container audit record has a fixed header and, potentially, additional event-specific data.

The container audit record header (audit_container_rcd_hdr) is a fixed structure that contains data for each audit event in the container audit file. Table A-6 shows the contents of the container audit record header.

Table A-6
Container Audit Record Header

Type	Identifier	Description
uint16	replicaNumber	NDS replica that generated the record.
uint16	eventTypeID	Container audit event type from Table A-7 or Table A-8.
uint16	recordNumber	Sequence number as generated by originating server within the current audit file.
uint32	dosDateTime	DOS-format date and time of audit event.
uint32	userID	NDS User object ID.
uint32	processUniqueID	Client process ID. This value can be used to trace client events (for example, file opens) to a specific process on that client. For the A_EVENT_RENAME_ENTRY and A_EVENT_MOVE_ENTRY records, the processUniqueID header field is used to identify the new object ID of the renamed or moved object. Thus, for these two events, the processUniqueID field cannot be used to trace the event to a specific process on the client.
uint32	successFailureStatusCode	Completion status: 0=successful, negative=failure.

Table A-7 defines each container event type (event number and record name), describes the event, and lists the format of any additional event-specific data in the audit record. The following defines the data types used in the third column of the table:

- LONG: A four-byte integer value.
- INT: A two-byte integer value.
- BYTE: A one-byte integer value.
- unicode: A null-terminated Unicode* (text) string.

The complete name of each event in Table A-7 starts with "ADS_"; that prefix is omitted to save room.

Table A-7
Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
101	ADD_ENTRY Audits the creation of a new object entry in NDS and any associated attributes (properties)of that object. If multiple attributes are created by this action, NDS writes an audit record for each attribute.	unicode; EntryName; RDN of new object entry unicode; AttrName; Name of attribute that is defined by creation of object (optional)
102	REMOVE_ENTRY Audit removal of an NDS object entry.	unicode; EntryName; RDN of removed object entry
103	RENAME_OBJECT Audit renaming of an NDS object.	(Note: DS sets the processUniqueID in the audit record header to object ID of the renamed object.) unicode; EntryName; new RDN for object unicode; oldEntryName; old RDN of object

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
104	MOVE_ENTRY Audit move of a leaf object to a new location in the tree.	(Note: NDS sets the processUniqueID in the audit record header to object ID of the moved object.) unicode; ObjectName1; Original RDN for object unicode; ObjectName2; New RDN for object
105	CHANGE_SECURITY_EQUIV Audit one or more changes to an object's Security Equals attribute.	unicode; EntryName; RDN of specified object entry unicode; ObjectName; RDN of object to which object EntryName is security equivalent (Note: The audit record will contain an additional ObjectName for each additional equivalence).
106	CHG_SECURITY_ALSO_EQUAL Audit one or more changes to an object's Security Also Equals attribute.	unicode; EntryName; RDN of specified object entry unicode; ObjectName; RDN of object to which EntryName can assume equivalent rights (Note: The audit record will contain an additional ObjectName for each additional equivalence).
107	CHANGE_ACL Audit one or more changes to an object's Access Control List. Each ACL item specifies an attribute of the current object, another object who has rights to that attribute, and the rights granted to the other object.	unicode; EntryName; RDN of specified object entry LONG; Privileges; Rights associated with access change unicode; ObjectName; RDN of object that is assigned rights to an attribute of the current object unicode; AttrName; Name of attribute (Note: The audit record will contain additional repetitions of Privileges, ObjectName, and AttrName for each additional ACL element.)

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
108	CHG_STATION_RESTRICTION Audit a change to Network Address Restriction property.	unicode; EntryName; RDN of user or printer object entry LONG; Nbytes; Number data bytes (10) BYTE; address[10]; IPX address restriction
109	LOGIN Audit a user's login to NDS.	LONG; UserID; User entry ID on server BYTE; NetworkAddrType; IPX=1 BYTE; NetworkAddrLen; Length; IPX uses 10 BYTE; NetworkAddress[ ]; IPX network address unicode; UserName[ ]; RDN of logged-in user.
110	LOGOUT Audit a user logout from NDS.	unicode; EntryName; RDN of logged out user
111	CHANGE_PASSWORD Audit a password change for the object. Note that the user password itself is not recorded.	unicode; EntryName; RDN of User object who changed password
112	USER_LOCKED Audit setting of the Locked by Intruder attribute of an NDS User object.	unicode; EntryName; RDN of locked user
113	USER_UNLOCKED Audit clearing the Locked by Intruder attribute of an NDS User object.	unicode; EntryName; RDN of unlocked user
114	USER_DISABLE Audit clearing of the Login Disabled attribute of an NDS User object.	unicode; EntryName; RDN of user that was disabled

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
115	USER_ENABLE Audit setting of the Login Disabled attribute of an NDS User object.	unicode; EntryName; RDN of user being enabled
116	CHANGE_INTRUDER_DETECT Audit a change to Login Intruder Limit setting for a container object (the container being audited).	LONG; Nbytes; Size of attribute Data[ ] array BYTE; Data[Nbytes]; New data for attribute unicode; AttrName; Name of intruder detection attribute (Note: The audit record will contain additional iterations of Nbytes, Data and AttrName for each additional intruder detection attribute.)
119	ADD_REPLICA Audits addition of a replica of an existing Directory partition to a server.	unicode; partName; RDN of the partition root unicode; serverName; RDN of server object LONG; replicaType; whether it's a Master, Read-Write, or Read-Only replica
120	REMOVE_REPLICA Audits removal of a replica from the replica set of an Directory partition	unicode; partName; RDN of the partition root unicode; serverName; RDN of server object
121	SPLIT_PARTITION Records splitting an Directory partition into two partitions at a specified object.	unicode; OldRootName; RDN of original partition root entry unicode; NewRootName; RDN of new partition root entry
122	JOIN_PARTITIONS Audit joining of a subordinate partition to its parent. (This event occurs twice in succession; first for the subordinate partition and then for the joined partition.)	unicode; EntryName; RDN of joined partition root.

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
123	CHANGE_REPLICA_TYPE Audit change to replica type of a given replica on a given server	LONG; oldType; previous replica type (Read Only, Secondary, Master) LONG; newType; new replica type unicode; entryname; RDN of partition root unicode; server name; RDN of server that holds the partition
124	REPAIR_TIME_STAMPS Audit setting object and object property timestamps for a replica to the local server time.	unicode; EntryName; RDN of partition root of the replica that was synchronized
126	ABORT_PARTITION_OP Audit termination of a repartitioning operation.	unicode; EntryName; RDN of partition root
127	SEND_REPLICA_UPDATES Audit transmission of an update to another Directory partition.	unicode; EntryName; RDN of replica root that sent updates
128	RECEIVE_REPLICA_UPDATES Audit receipt of an update from another Directory partition.	unicode; EntryName; RDN of replica root that received updates
129	ADD_MEMBER Records creating an object using Bindery emulation.	unicode; ObjectName; RDN of object entry LONG; MemberID; ID of member having rights to property unicode; PropertyName; Name of bindery property
130	BACKUP_ENTRY Records backing up an NDS object, including its attributes.	unicode; EntryName; RDN of NDS object

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
131	CHANGE_BIND_OBJ_SECURITY Records a change to a Bindery object's access rights through Bindery emulation.	unicode; ObjectName; Name of Bindery object LONG; ObjectSecurity; Bindery access level Read (0-4), Write (0-4)
132	CHANGE_PROP_SECURITY Records a change to a Bindery property's access rights through Bindery emulation.	unicode; PropertyName; Bindery property name LONG; PropertySecurity; Bindery access level Read (0-4), Write (0-4)
133	CHANGE_TREE_NAME Records renaming an NDS tree. The audit record is logged in the audit file of the Root container for the Directory tree.	unicode; NewTreeName; Name of the Directory tree
134	CHECK_CONSOLE_OPERATOR Records a client's request to check it's console rights. The audit record is associated with the user identified in the audit record header.	unicode; ServerName; RDN of server object unicode; UserName; Name of user being checked for console rights LONG; isOperator; Flag identifying console rights: zero (not console operator), non-zero (is a console operator)
135	COMPARE_ATTR_VALUE Records a comparison of a client-supplied value to the value of a property in NDS.	unicode; EntryName; Name of object entry for which attribute is being compared unicode; AttrName; Name of specified attribute
136	CREATE_PROPERTY Records creating a property of a Bindery object through bindery emulation.	unicode; ObjectName; Name of Bindery object unicode; PropertyName; Name of Bindery property LONG; PropertySecurity; Bindery access level Read (0-4), Write (0-4)

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
137	CREATE_SUBORDINATE_REF Records adding a subordinate reference to the parent partition.	unicode; EntryName; RDN of parent partition root entry
138	DEFINE_ATTR_DEF Records defining a new attribute in the NDS schema.	unicode; AttrName; Name of new attribute
139	DEFINE_CLASS_DEF Records defining a new object class in the NDS schema.	unicode; ClassName; Name of new object class
140	DELETE_MEMBER Records deleting an object through bindery emulation.	unicode; ObjectName; RDN of object entry LONG; MemberID; ID of member having rights to property unicode; PropertyName; Name of bindery property
141	DELETE_PROPERTY Records deleting a property of a Bindery object through bindery emulation.	unicode; ObjectName; Name of Bindery object unicode; PropertyName; Name of bindery property
142	DS_NCP_RELOAD Records restarting NDS.	(None)
143	RESET_DS_COUNTERS Records resetting the NDS counters.	unicode; ServerName; RDN of specified server object
144	FRAG_REQUEST Records a fragmented request to a server.	(None)

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
145	INSPECT_ENTRY Records querying an NDS object for partition status and other information.	unicode; EntryName; RDN of queried object
146	LIST_CONTAINABLE_CLASSES Records retrieving the set of object classes that can be subordinate to an object.	unicode; EntryName; RDN of specified object
147	LIST_PARTITIONS Records listing the Directory partitions on a server.	unicode; PartitionRootName; RDN of partition root entry
148	LIST_SUBORDINATES Records retrieving the subordinate objects to an object.	unicode; EntryName; RDN of specified object
149	MERGE_TREE Records merging two Directory trees.	(None)
150	MODIFY_CLASS_DEF Records modification of an NDS class definition in the schema.	unicode; ClassName; Name of modified class definition
151	MOVE_TREE Records moving a portion of the Directory tree.	unicode; SrcParentName; RDN of source container name of the root of the subtree. unicode; DestParentName; RDN of destination container name of the root of the subtree.
152	OPEN_STREAM Records opening a stream property of an NDS object.	unicode; EntryName; RDN of NDS object unicode; AttrName; Name of NDS attribute unicode; DesiredRights; Object property rights for stream file

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
153	READ Records reading one or more properties of an NDS object.	unicode; EntryName; RDN of object entry unicode; AttrName; Name of attribute to be read
154	READ_REFERENCES Records retrieving the list of references for an object.	unicode; EntryName; RDN of requested object
155	REMOVE_ATTR_DEF Records removing an attribute definition from the NDS schema.	unicode; AttrName; Name of removed attribute definition
156	REMOVE_CLASS_DEF Records removing a class definition from the NDS schema.	unicode; ClassName; Name of removed class definition
157	REMOVE_ENTRY_DIR Records removing the queue directory from an NDS object.	unicode; EntryName; RDN of NDS object for which queue directory was removed
158	RESTORE_ENTRY Records restoring an NDS entry and its attributes from a backup.	unicode; EntryName; RDN of restored entry
159	START_JOIN Records the beginning of a tree join operation.	unicode; ParentRootEntryName; RDN of root object (container) that is parent of joined tree unicode; ChildRootEntryName; RDN of root object that is joined as a child
160	START_UPDATE_REPLICA Records starting to update a replica from another server.	unicode; ReplicaName; RDN of root object for replica
161	START_UPDATE_SCHEMA Records starting to update the schema from another server.	unicode; ClientServerName; RDN of server object

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
162	SYNC_PARTITION Records a request by a server to synchronize a partition with another server.	unicode; PartitionDistName; RDN of root object of partition
163	SYNC_SCHEMA Records a request by a server to synchronize its schema with another server.	(None)
164	UPDATE_REPLICA Records making updates to a replica as a result of a skulk from another server.	unicode; ReplicaName; RDN of root object of replica that is updated
165	UPDATE_SCHEMA Records making updates to the schema as a result of a skulk from another server.	unicode; ClientServerName; RDN of server object
166	VERIFY_PASSWORD Records an attempt to verify a user's password.	unicode; EntryName; RDN of specified User object entry
167	ABORT_JOIN Records a failed attempt to join Directory partitions.	unicode; ParentRootEntryName; RDN of root object (container) that was to be parent of joined tree unicode; ChildRootEntryName; RDN of root object that was to be joined as a child
168	RESEND_ENTRY Records an attempt to resend an NDS update.	unicode; EntryName; RDN of object to be replicated

Table A-7 *continued*

Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
169	MUTATE_ENTRY Records a change to an NDS object's class.unicode; EntryName; RDN of object to be changed	unicode; NewClassName; Name of object's new class
170	MERGE_ENTRIES Records a merger of two NDS containers.	unicode; WinnerEntry; RDN that continues to exist in merged container unicode; LoserEntry; RDN that loses its identity after being merged.
171	END_UPDATE_REPLICA Records completion of replica update	unicode; EntryName; RDN of root object of replica
172	END_UPDATE_SCHEMA Records completion of schema update.	unicode; EntryName; RDN of server object.
173	CREATE_BACKLINK Records creation of a back pointer to an NDS object on another server.	unicode; EntryName; RDN of NDS object entry.
174	MODIFY_ENTRY Records modification of an NDS object entry and (potentially) an attribute of that object. If multiple attributes are modified by this action, NDS writes an audit record for each attribute.	unicode; EntryName; RDN of object unicode; AttrName; Name of attribute that is modified (optional)
176	NEW_SCHEMA_EPOCH Records changes to the schema epoch.	(None)
177	CLOSE_Bindery Records that bindery was closed	(None)

Table A-7 *continued*
Container Audit Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
178	OPEN_BINDERY Records that bindery was opened	(None)

The container audit history events are defined in Table A-8. Audit events marked with a (*) in that table will not occur in the NetWare® Enhanced Security configuration, because passwords are not used for access control. The complete name of each event in Table A-8 starts with "AUDITING_"; that prefix is omitted to save room.

Table A-8
Container Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
58	ACTIVE_CONNECTION_RCD Records establishment of an active connection. This is the means used to associate a user's identity with subsequent operations on a connection. After an audit file is reset, active connections are written to new audit file.	LONG; UserID; User entry ID on server BYTE; NetworkAddrType; IPX=1 BYTE; NetworkAddrLen; Length (IPX uses 10) BYTE; NetworkAddress; IPX network address BYTE; Name[ ]; Length-preceded username
59 (*)	ADD_AUDITOR_ACCESS Records an auditor gaining access to audit trail by providing the password.	LONG; UserID; User entry ID on server BYTE; NetworkAddrType IPX=1 BYTE; NetworkAddrLen; Length (IPX uses 10) BYTE; NetworkAddr; IPX network address BYTE; Name[ ]; Length-preceded username
61 (*)	CHANGE_AUDIT_PASSWORD Records a change to level 1 password.	(None)

Table A-8 *continued*

Container Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
66	REMOVE_AUDITOR_ACCESS Records an auditor relinquishing access to the audit trail.	(None)
67	RESET_AUDIT_FILE Records an auditor resetting (rolling over) to a new audit file. Appears as both the last record of the old audit file and the first record of the new audit file.	(None)
71	WRITE_AUDIT_CONFIG_HDR Records write of configuration data to audit file header.	(None)
74 (*)	CHANGE_AUDIT_PASSWORD2 Generated when level 2 password is changed.	(None)
77 (*)	INTRUDER_DETECT Generated when a user fails log in to an audit file because the incorrect password was provided.	LONG; UserID; User entry ID on server BYTE; NetworkAddrType; IPX=1 BYTE; NetworkAddrLen; Length (IPX uses 10) BYTE; NetworkAddr; IPX network address BYTE; Name[ ]; Length-preceded username
81	DELETE_OLD_AUDIT_FILE Records deletion of an old audit file.	(None)
82	QUERY_AUDIT_STATUS Records gaining access to the audit file.	(None)

Table A-8 *continued*
Container Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
91	DISABLE_CNT_AUDIT Generated when auditing is disabled for a container.	(None)
92	ENABLE_CNT_AUDITING Generated when auditing is enabled for a container.	(None)
93	NULL_RECORD Dummy record to replace CLOSE_CNT_AUDITING in skulked copies of the audit trail.	(None)

Table A-8 *continued*

Container Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
94	CLOSE_CNT_AUDITING Records that audit recording was stopped as a result of DS halting or audit disabling. The last five event-specific data items are repeated for each server in the replica ring. One or more CLOSE_CNT_AUDITING records are generated when a container audit trail is closed. The event specific data includes the FirstReplicaEntryIndex, the LastReplicaEntryIndex, and from 1 to 32 instances of a structure containing RecordNumber, FileOffset, ReplicaNumber, SkulkNeeded, and SkulkSkipCount. The first CLOSE_CNT_AUDITING record has information about the first 32 replicas (thus FirstReplicaEntryIndex is 0 and LastReplicaEntryIndex is 31; the second CLOSE_CNT_AUDITING record will have information about the next 32 replicas (thus FirstReplicaEntryIndex will be 32 and LastReplicaEntryIndex will be 62), etc.	LONG; FirstReplicaEntryIndex; Index in replica table of first replica of container LONG; LastReplicaEntryIndex; Index in replica table of last replica of container LONG; RecordNumber; Number of last record in audit file LONG; FileOffset; Offset of end of audit file INT ReplicaNumber; Number (as opposed to index) of first replica of container. BYTE; SkulkNeeded; Skulk control flag BYTE; SkulkSkipCount; indicates whether audit skulking for the replica succeeded or failed
95	CHANGE_USER_AUDITED Records setting or clearing the per-user audit flag used for volume auditing.	BYTE; Name[ ]; Length-preceded username that was changed

Table A-8 *continued*
Container Audit History Records

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
98	CONTAINER_NAME_RCD2 Generated at beginning of container audit file. Includes the class name (for example, “Organizational Unit") and container name.	unicode; SchemaClassName; Class name of container object as defined in schema unicode; ContainerDN; DN of container being audited

Events 58 (AUDITING_ACTIVE_CONNECTION_RCD) and 98 (AUDITING_CONTAINER_NAME_RCD2) are pseudo-events (that is, they do not represent actual events).

Pseudo-events are used so that each audit data file can be self-contained. If a user logs in, event 109 (ADS_LOGIN) is generated (as shown in Table A-7). If a subsequent audit reset occurs, the pseudo-event 58 would be generated for each logged in user, so the new audit data file would have a record of all logged in users (thus making subsequent references in the audit file to connection numbers meaningful).

Event 98 is always the first audit event in each container audit file, recording the container which caused generation of the audit file.

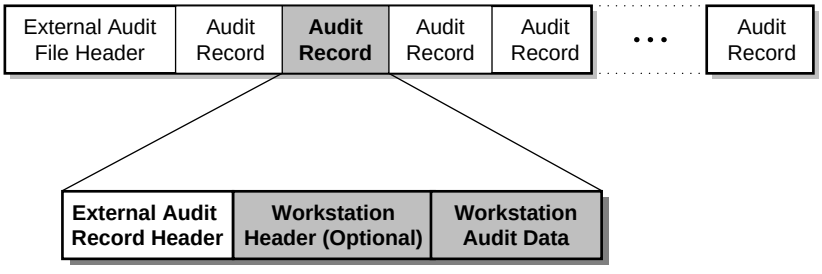
Textual Audit Format (AUDITCON)

There is a one-to-one correspondence between the binary audit record format and the textual representation of the event. Refer to “View Audit File” on page 190 and “View Audit History” on page 193 for examples of the AUDITCON report format.

External Audit Format

As shown in Figure A-1, external audit files consist of an audit file header and a sequence of audit records. Audit records can be either generated by the server (audit history records) or inserted by external entities (external audit records).

Figure A-1
Structure of External Audit Record



The external audit record data (shaded) consists of an external audit record header generated by NetWare, followed by a sequence of bytes. The workstation provided data can be interpreted by the workstation in any way that is desired.

For example, a workstation product can treat this data as a workstation event header (for example, that lists the time the event occurred on the workstation and the workstation's audit record type) and additional data. See your vendor's workstation documentation for information on the workstation data in your external audit file.

Warning

The external audit record header contains information written by the server at the time the audit event record is written to the audit file, for example, the date and time the event was recorded. Depending upon the workstation's audit architecture, this information might or might not be meaningful.

For example, the workstation might queue audit records for a period of time before uploading the records to the server to be written to the audit file. If the information in the external audit record header is not sufficient for an auditor to audit the actions of an individual user, then the workstation NTCB partition must record additional data in the workstation data.

External Audit File Header

The external audit file header is the same as the container audit file header defined in the section "Container Audit File Header" on page 292.

External Audit Record Format

This section defines the binary format of each audit record in the external audit trail. Each audit record has a fixed header and, potentially, additional event-specific data.

Table A-9 lists the subset of the event record types and formats described in Table A-8 that are possible in an external audit trail. In addition, the table shows the events that can appear in an external audit trail that can not appear in container audit trails.

Table A-9
Event Types in an External Audit Trail

Event Number	Description
66	AUDITING_REMOVE_AUDITOR_ACCESS
67	AUDITING_RESET_AUDIT_FILE
71	AUDITING_WRITE_AUDIT_CONFIG_HDR
81	AUDITING_DELETE_OLD_AUDIT_FILE
82	AUDITING_QUERY_AUDIT_STATUS
91	AUDITING_DISABLE_CNT_AUDIT
92	AUDITING_ENABLE_CNT_AUDITING
98	AUDITING_CONTAINER_NAME_RCD2

Table A-10
External Audit Event Types

Event Number	Record Name Description and Comments	Additional Event-Specific Data (Type; Declaration; Description)
97	EXTERNAL_RECORD	LONG; VendorID; Novell assigned ID
	Audit record generated by an external source and inserted in the audit trail.	LONG; RecLen; Record length in bytes
		BYTE; Data[RecLen]; Externally supplied audit record

The external audit record header (audit_external_rec_hdr) is a fixed structure that contains data for each audit event in the external audit file. Table A-11 shows the contents of the external audit record header.

Table A-11
External Audit Record Header

Type	Element Name	Description
uint16	replicaNumber	Unused.
uint16	eventTypeID	Container audit event type from Table A-9
uint16	recordNumber	Sequence number.
uint32	dosDateTime	DOS-format date and time of audit event.
uint32	userID	NDS User object ID.
uint32	processUniqueID	Client process ID. This value can be used to trace client events (for example, file opens) to a specific process on that client.
uint32	successFailureStatusCode	Completion status: 0=successful, negative=failure.

Trademarks

Novell, Inc. has attempted to supply trademark information about company names, products, and services mentioned in this manual. The following list of trademarks was derived from various sources.

Novell Trademarks

NetWare is a registered trademark of Novell, Inc. in the United States and other countries.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

Novell Directory Services and NDS are trademarks of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

Novell is a registered trademark of Novell, Inc. in the United States and other countries.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

Third-Party Trademarks

DynaText is a registered trademark of Electronic Book Technologies, Inc.

OS/2 is a registered trademark of International Business Machines Corporation.

Unicode is a registered trademark of Unicode, Inc.

Windows is a registered trademark of Microsoft Corporation.

Index

A

B

C

D

E

F

G

I

L

N

O

P

R

S

T

U

V

User Comments

We want to hear your comments and suggestions about this manual. Please send them to the following address:

Novell, Inc.
Documentation Development
MS C-23-1
122 East 1700 South
Provo, UT 84606
U.S.A

Fax: (801) 861-3002

IntranetWare
Auditing the Network
Part #Place Part Number Here
June 1997

For technical support issues, contact your local dealer.

Your name and title: _____

Company: _____

Address: _____

_____

_____

Phone number: _____ Fax: _____

I use this manual as ❑ an overview ❑ a tutorial ❑ a reference ❑ a guide ❑ _____

	Excellent	Good	Fair	Poor
Completeness	❑	❑	❑	❑
Readability (style)	❑	❑	❑	❑
Organization/Format	❑	❑	❑	❑
Accuracy	❑	❑	❑	❑
Examples	❑	❑	❑	❑
Illustrations	❑	❑	❑	❑
Usefulness	❑	❑	❑	❑

Please explain any of your ratings: _____

_____

_____

_____

_____

In what ways can this manual be improved? _____

_____

_____

_____

_____

You may photocopy this comment page as needed so that others can also send in comments.