VMS

VMS Audit Analysis Utility Manual

Order Number: AA–NG63A–TE

VMS Audit Analysis Utility Manual

Order Number: AA–NG63A–TE

June 1989

This document describes how to use the Audit Analysis Utility on VMS operating systems.

Revision/Update Information:	This is a new document.
Software Version:	VMS Version 5.2

digital equipment corporation
maynard, massachusetts

June 1989

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

The software described in this document is furnished under a license and may be used or copied only in accordance with the terms of such license.

No responsibility is assumed for the use or reliability of software on equipment that is not supplied by Digital Equipment Corporation or its affiliated companies.

The postpaid Reader's Comments forms at the end of this document request your critical evaluation to assist in preparing future documentation.

The following are trademarks of Digital Equipment Corporation:

CDA
DDIF
DEC
DECnet
DECUS
DECwindows
DIGITAL
LN03
MASSBUS
PrintServer 40
Q-bus
ReGIS
ULTRIX
UNIBUS
VAX
VAXcluster
VAX RMS
VAXstation
VMS
VT
XUI
digital™

The following is a third-party trademark:

PostScript is a registered trademark of Adobe Systems, Inc.

ZK5214

Production Note

This book was produced with the VAX DOCUMENT electronic publishing system, a software tool developed and sold by Digital. In this system, writers use an ASCII text editor to create source files containing text and English-like code; this code labels the structural elements of the document, such as chapters, paragraphs, and tables. The VAX DOCUMENT software, which runs on the VMS operating system, interprets the code to format the text, generate a table of contents and index, and paginate the entire document. Writers can print the document on the terminal or line printer, or they can use Digital-supported devices, such as the LN03 laser printer and PostScript printers (PrintServer 40 or LN03R ScriptPrinter), to produce a typeset-quality copy containing integrated graphics.

Contents

EXAMPLES

FIGURES

TABLES

Preface

Intended Audience

This manual is intended for VMS system managers, site security administrators, operators, and system programmers.

Document Structure

This document consists of the following sections:

- The first section provides a full description of the Audit Analysis Utility.
- The second section outlines the following ANALYZE/AUDIT information:
    - Invoking the utility
    - Exiting from the utility
    - Directing output
    - Restrictions or privileges required
- The following section describes ANALYZE/AUDIT qualifiers, including format, parameters, and examples.
- The final section describes Interactive Mode Commands
- Appendix A describes the format of a security audit record.

Associated Documents

You should be familiar with the basic security concepts described in the *Guide to VMS System Security*.

Conventions

The following conventions are used in this manual:

CTRL/x

A sequence such as CTRL/x indicates that you must hold down the key labeled CTRL while you press another key or a pointing device button.

PF1 x

A sequence such as PF1 x indicates that you must first press and release the key labeled PF1, then press and release another key or a pointing device button.

Return

A key name is shown enclosed to indicate that you press a key on the keyboard.

. . .

In examples, a horizontal ellipsis indicates one of the following possibilities:

- Additional optional arguments in a statement have been omitted.
- The preceding item or items can be repeated one or more times.
- Additional parameters, values, or other information can be entered.

.
.
.

A vertical ellipsis indicates the omission of items from a code example or command format; the items are omitted because they are not important to the topic being discussed.

()

In format descriptions, parentheses indicate that, if you choose more than one option, you must enclose the choices in parentheses.

[]

In format descriptions, brackets indicate that whatever is enclosed is optional; you can select none, one, or all of the choices.

{}

In format descriptions, braces surround a required choice of options; you must choose one of the options listed.

red ink

Red ink indicates information that you must enter from the keyboard or a screen object that you must choose or click on. For online versions, user input is shown in **bold**.

boldface text

Boldface text represents the introduction of a new term or the name of an argument, an attribute, or a reason.

italic text

Italic text represents information that can vary in system messages (for example, Internal error *number*).

UPPERCASE TEXT

Uppercase letters indicate that you must enter a command (for example, enter OPEN/READ).

UPPERCASE TEXT

Uppercase letters indicate the name of a routine, the name of a file, the name of a file protection code, or the abbreviation for a system privilege.

-

Hyphens in coding examples indicate that additional arguments to the request are provided on the line that follows.

numbers

Unless otherwise noted, all numbers in the text are assumed to be decimal. Nondecimal radixes—binary, octal, or hexadecimal—are explicitly indicated.

ANALYZE/AUDIT Description

The Audit Analysis Utility (ANALYZE/AUDIT) is a new system management tool that enables system managers and site security administrators to selectively extract and display information from security audit log files or security archive files. Using ANALYZE/AUDIT qualifiers, you can produce audit analysis reports in a variety of formats and select specific audit events to be included in the report.

Note: **The Audit Analysis Utility replaces the SECAUDIT.COM command procedure that was included in previous versions of the VMS operating system.**

You can use ANALYZE/AUDIT to produce audit analysis reports in one of the following forms:

- A brief (one line per record) listing (/BRIEF)
- A full listing (/FULL)
- A summary of all security events processed (/SUMMARY)
- A binary output file (/BINARY)

You can use the brief output format from the Audit Analysis Utility to perform a daily inspection of the security audit log file. If any of the selected events arouse your suspicion, you can produce a full-format listing of selected events and perform a more complete inspection of the data, as described in Section 3.

You can specify the following qualifiers with the ANALYZE/AUDIT command to determine the criteria used to create an audit analysis report:

- /BEFORE and /SINCE extract security events logged during a specific period of time.
- /EVENT_TYPE lists all security event messages of a specific event class.
- /SELECT and /IGNORE produce a listing that includes or excludes security event messages based upon the fields contained in the messages. (For example, /SELECT=USERNAME=JSNOOP lists only security event messages generated by user JSNOOP.)

Use the SET AUDIT command to enable and disable the recording of specific audit events in the system security audit log file and to modify characteristics of the audit server; use the SHOW AUDIT command to display the list of system events for which auditing is enabled. The *VMS DCL Dictionary* provides complete descriptions of the DCL commands SET AUDIT and SHOW AUDIT.

1 ANALYZE/AUDIT Command Line Format

Use the DCL command ANALYZE/AUDIT to perform audit analysis operations on security audit log files or security archive files. An ANALYZE/AUDIT command can specify the name of one or more log files, as follows:

```
ANALYZE/AUDIT [file-spec,...]
```

If you omit the **file-spec** parameter, an attempt is made to perform audit analysis on the file SECURITY_AUDIT.AUDIT$JOURNAL in the current directory. (SECURITY_AUDIT.AUDIT$JOURNAL is the name of the system security audit log file created, by default, in the SYS$COMMON:[SYSMGR] directory.)

In addition to the system security audit log file, you can use the ANALYZE/AUDIT command to extract security event messages from binary files created with previous ANALYZE/AUDIT commands, as well as from security archive files. See the *Guide to VMS System Security* for information about creating a security archive file.

2 Audit Analysis Utility Output

You can specify a number of different forms of output from the Audit Analysis Utility: brief listing (the default), full listing, summary report, and binary output.

By default, the output is directed to SYS$OUTPUT. However, you can specify an output file with the /OUTPUT qualifier. You can further specify whether the output should be in binary or ASCII format with the /BINARY qualifier. If you specify /BINARY, a binary audit analysis file is produced that can later be processed using other audit analysis commands. If you accept the default brief output format (/BRIEF) or request a full format (/FULL) or summary (/SUMMARY) display, an ASCII file is produced.

2.1 Brief Listing Format

The brief listing format provides one line for each record in the audit log file being processed. As shown in Example AUD–1, a brief output always includes date and time, type of record, subtype, node name, user name, process ID, and terminal.

Use the following command to produce a brief report of all the security audit events logged to the system security audit log file:

```
$ ANALYZE/AUDIT SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

Note that because the brief listing format is the default output type, the /BRIEF qualifier is not required.

Example AUD–1 Sample Brief Listing

```
     Date / Time            Type        Subtype       Node    Username      ID     Term
-------------------------------------------------------------------------------------
1-NOV-1989 16:00:03.37 ACCESS     FILE_ACCESS      HERE   SYSTEM       5B600AE4
1-NOV-1989 16:00:59.66 LOGIN      SUBPROCESS       GONE   PIPERSKI     3BA011D4
1-NOV-1989 16:02:37.31 LOGIN      SUBPROCESS       GONE   MILANT       000000D5
1-NOV-1989 16:06:36.40 LOGFAIL    LOCAL            SUPER  MBILLS       000000E5 _TTA1:
  .
  .
  .
```

2.2 Full Listing Format

The full listing format provides all the data for each record in the audit journal file being processed. There are small variations in record formats, based on the presence or absence of data in the record. Example AUD–2 displays a single audit analysis record in the full format. You can produce full format audit analysis reports with the following command:

```
$ ANALYZE/AUDIT/FULL SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

Example AUD–2 Sample Full Listing

```
Security alarm (SECURITY) and security audit (SECURITY) on CANINE, system id: 19681
Auditable event:        Local interactive login failure
Event time:              1-NOV-1989 19:06:36.40
PID:                    000000D6
Username:               PGEORGE
Terminal name:          _LTA2: (ZK34C2/LC-2-15)
Status:                 %LOGIN-F-INVPWD, invalid password
```

2.3 Summary Report Format

A summary report lists the total number of audit messages generated throughout the ANALYZE/AUDIT period for each class of security event. The summary report provides you with a method of quickly identifying potential security problems.

Example AUD–3 illustrates a summary output for the following command:

```
$ ANALYZE/AUDIT/SUMMARY
```

Example AUD–3 Sample Summary Output

```
Total records read:     6315           Records selected:       6315
Record buffer size:     512            Format buffer size:     128
Server messages:        0              Customer messages:      0
Digital CSS messages:   0              Layered prod messages:  0
Audit changes:          40             Installed db changes:   54
Login failures:         22             Breakin attempts:       1
Successful logins:      560            Successful logouts:     347
System UAF changes:     5              Network UAF changes:    0
Rights db changes:      0              Object accesses:        5111
Volume (dis)mounts:     176
```

You can produce a summary report by itself, as shown in the previous example, or in combination with a brief or full format audit analysis report, as shown in the following command:

```
$ ANALYZE/AUDIT/BRIEF/SINCE=TODAY/SUMMARY/OUTPUT=TODAY.LIS -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example creates a file named TODAY.LIS containing a brief listing of all security audit messages generated since midnight of the current day followed by a summary of all the records generated.

2.4 Binary Output

To create a binary output file, specify the /BINARY qualifier with the ANALYZE/AUDIT command. The binary file contains a set of the audit records from the input (source) audit log files. Your selection criteria determines the set of records included in the binary file. You can use binary output files as source files for future audit analysis requests.

When using the /BINARY qualifier, all records that match the selection criteria are written to the binary output file.

A complete description of the audit message record format appears in Appendix A.

3 How to Perform an Audit Analysis

This section describes how to perform a successful audit analysis of your system. Although the way you use the VMS Audit Analysis Utility will depend upon the security needs at your site, there are a number of common steps that you should follow, regardless of the extent to which you use the Audit Analysis Utility:

- Before you begin producing audit analysis reports, familiarize yourself with the normal operation of your system. Understand what types of security events are generated as part of normal system operation. This knowledge will enable you to determine when to suspect a security problem and when to disregard system security events as uninteresting or irrelevant.

- Develop a procedure for generating and reviewing audit analysis reports on a periodic basis in order to determine which security events logged to the audit journal warrant a more thorough investigation.

- Perform a detailed investigation of selected security events when your regular audit analysis leads you to suspect a security problem.

3.1 Recognizing Common System Events

Before using the Audit Analysis Utility, you should become as familiar as possible with the ways in which your system is normally used. This will enable you to more easily distinguish between a security event message that requires further investigation and one that can be ignored.

As a system manager, you should be able to answer the following questions before performing an audit analysis:

- What are the typical hours of operation for most users of the system?
- Are there specific users who normally operate with advanced privileges?
- Which images generate system security events as part of other applications?
- Are there any regular batch or network jobs that run at specific times of the day?

By knowing the answers to these questions, you can eliminate false alarms, which otherwise may have caused you to wrongly suspect a security problem.

At this point, you are ready to generate routine audit analysis reports to monitor security activity on your system.

3.2 Performing a Periodic Audit Analysis

While it is possible to generate a wide variety of audit analysis reports, the most common type of report that you will probably generate is the daily listing. Typically, you might create a command procedure that runs in a batch job every evening before midnight to generate a report of the day's security event messages. The following example shows the ANALYZE/AUDIT command you would use to generate this report:

```
$ ANALYZE/AUDIT/SINCE=TODAY/OUTPUT=31DEC1989.AUDIT -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
$ MAIL/SUBJECT="Security Events" 31DEC1989.AUDIT SYSTEM
```

The first command in this example produces a file named 31DEC1989.AUDIT, which contains all the security event messages generated during the current day. The second command sends the file to the system manager for examination. By default, the report is produced using the brief (one line) format.

An alternate method of producing a daily audit analysis report is to generate a full format listing of selected security audit records, as shown in the following example:

```
$ ANALYZE/AUDIT/FULL/SINCE=TODAY/OUTPUT=31DEC1989.AUDIT -
_$ /EVENT_TYPE=(BREAKIN,NETUAF,RIGHTSDB,SYSUAF)
$ MAIL/SUBJECT="Security Events" 31DEC1989.AUDIT SYSTEM
```

It is important that you review audit analysis reports as soon as possible. The sooner you inspect the reports, the sooner you become aware of any possible breach of security on the system and determine the extent of the problem. You can make the inspection of the previous day's audit analysis report a regular part of your morning routine, or you can create a program that reviews the report and notifies you through Mail when suspicious events have been found.

3.3 Performing a Detailed Audit Analysis

When a routine audit analysis leads you to suspect that the security of your system has been compromised—through an actual or attempted breakin, repeated login failures, or any other suspicious security events—you can investigate the source of the security event through a more detailed inspection of the security audit log file.

For example, suppose that you see the security events shown in Example AUD–4 during a routine inspection of the previous day's audit analysis report:

Example AUD–4 Spotting Suspicious Activity in the Audit Analysis Report

```
      Date / Time          Type         Subtype       Node    Username      ID     Term
----------------------------------------------------------------------------------------
   .
   .
   .
26-OCT-1989 16:06:09.17 LOGFAIL    REMOTE           BOSTON JGARNER     5BC002EA _RTA14:
26-OCT-1989 16:06:22.01 LOGFAIL    REMOTE           BOSTON JGARNER     5BC002EA _RTA14:
26-OCT-1989 16:06:34.17 LOGFAIL    REMOTE           BOSTON JGARNER     5BC002EA _RTA14:
26-OCT-1989 16:06:45.50 LOGFAIL    REMOTE           BOSTON JGARNER     5BC002EA _RTA14:
26-OCT-1989 16:07:12.39 LOGIN      REMOTE           BOSTON JGARNER     5BC002EA _RTA14:
26-OCT-1989 16:23:42.45 SYSUAF     SYSUAF_ADD       BOSTON JGARNER     5BC002EA _RTA14:
   .
   .
   .
```

The security events displayed in this report indicate that user JGARNER logged in to the system following four unsuccessful login attempts. Shortly after logging in, user JGARNER created a new account in the system user authorization file (SYSUAF).

At this point, you must determine whether this behavior is normal or abnormal. Is user JGARNER authorized to add new user accounts to the system? If you believe that the security of your system has been compromised, perform a more detailed examination of the security audit log file to determine if damage has been done to your system, as shown in the following command:

```
$ ANALYZE/AUDIT/FULL/SINCE=26-OCT-1989:16:06
```

The command in this example generates a full format listing of all security audit events copied to the audit log file since user JGARNER first attempted to log in to the system. In full format, all the data available for each record in the audit log file is displayed. Using the previous command, you can find out the name of the remote user who logged in under the local JGARNER account and the node from which the login was made, as shown in Example AUD–5.

Example AUD–5 A Full Format Audit Analysis Report

```
   .
   .
   .
Security alarm (SECURITY) and security audit (SECURITY) on BOSTON, system id: 19941
Auditable event:        Remote interactive login failure
Event time:             26-OCT-1989 16:06:09.17
PID:                    5BC002EA
Username:               JGARNER
Terminal name:          _RTA14:
Remote nodename:        NASHWA         Remote node id:         7300
Remote username:        FOLEY
Status:                 %LOGIN-F-INVPWD, invalid password
   .
   .
   .
```

The information displayed in this example indicates that the login failures and subsequent successful login were made by user FOLEY from the remote node NASHWA. Your next step is to determine whether the security events were generated by user FOLEY or by someone who has broken into the remote node NASHWA through the FOLEY account.

3.4 Using Interactive Mode Commands

The Audit Analysis Utility offers an alternative method of analyzing system security events logged to the system security audit log file: interactive command mode. At any time during a full or brief audit analysis listing, you can interrupt the report being displayed and enter interactive command mode by using the CTRL/C key combination, as shown in Example AUD–6:

Example AUD–6 Entering Interactive Command Mode

```
      Date / Time          Type        Subtype       Node    Username      ID    Term
-----------------------------------------------------------------------------------
   .
   .
   .
09-DEC-1989 10:25:09.17 LOGFAIL    REMOTE           THERCK MINTICK      4AD003AB _RTA99
09-DEC-1989 10:25:22.01 LOGFAIL    REMOTE           THERCK MINTICK      4AD003AB _RTA99
09-DEC-1989 10:25:34.17 LOGFAIL    REMOTE           THERCK MINTICK      4AD003AB _RTA99
09-DEC-1989 10:25:45.50 LOGFAIL    REMOTE           THERCK MINTICK      4AD003AB _RTA99
16-DEC-1989 09:01:52.11 LOGFAIL    REMOTE           ALGONE MORRIS       2640020A _RTA11
   .
   .
   .
CTRL/C
COMMAND>
```

At the *COMMAND>* prompt, you can enter interactive mode commands to generate a new audit analysis report using a different set of audit analysis criteria or to reposition yourself within the security audit log file. Then, enter the CONTINUE command to return to the full or brief audit analysis listing, or use the EXIT command to terminate the report and return to the DCL command level. See the interactive mode command section for a complete list of all interactive mode commands.

Online Help

The Audit Analysis Utility provides a Help facility that contains information about all interactive mode commands. Enter the HELP command at the *COMMAND>* prompt for descriptions of each interactive mode command.

ANALYZE/AUDIT Usage Summary

The Audit Analysis Utility (ANALYZE/AUDIT) processes security audit messages to produce reports and summaries of security events on the system.

FORMAT

ANALYZE/AUDIT *[file-spec[,...]]*

Parameter

file-spec[,...]
Specifies one or more security audit log files as input to be processed by the Audit Analysis Utility. If you specify more than one file name, separate them with commas. If your current directory is the system manager directory and you omit the **file-spec** parameter, data is processed from the default security audit log file, SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL.

Wildcard characters are allowed in the file specification.

usage summary

The following DCL command invokes the Audit Analysis Utility:

```
ANALYZE/AUDIT [file-spec[,...]]
```

Each ANALYZE/AUDIT request runs until it completes. To terminate an ANALYZE/AUDIT request before completion, press CTRL/Z.

You can direct ANALYZE/AUDIT output to any supported terminal device or to a disk or tape file by specifying the /OUTPUT qualifier.

Note: **Use of the Audit Analysis Utility requires no special privileges other than access to the files specified on the command line.**

ANALYZE/AUDIT QUALIFIERS

This section describes qualifiers for the ANALYZE/AUDIT command and provides examples of their use. The qualifiers follow the standard rules of DCL grammar, as described in the *VMS DCL Concepts Manual.*

/BEFORE

Controls whether records dated earlier than the specified time are selected.

FORMAT

/BEFORE*[=time]*
/NOBEFORE

KEYWORD

time

Specifies the time used to select records. Records dated earlier than the specified time are selected. You can specify an absolute time, delta time, or a combination of the two. Observe the syntax rules for date and time described in the *VMS DCL Concepts Manual.*

DESCRIPTION

By default, all records in the security audit log file may be examined. You must specify /BEFORE to discard records created after a specific point in time.

EXAMPLES

```
$ ANALYZE/AUDIT /BEFORE=25-NOV-1989 -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects all records dated earlier than November 25, 1989.

```
$ ANALYZE/AUDIT /BEFORE=14:00/SINCE=12:00 -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects all records generated between noon and 2 P.M. today.

/BINARY

Controls whether output is a binary file.

FORMAT

/BINARY
/NOBINARY

KEYWORDS

None.

DESCRIPTION

When /BINARY is specified, the output file, specified using the /OUTPUT qualifier, contains image copies of the selected input records. If you specify /NOBINARY or omit the qualifier, the output file contains ASCII records.

By default, if you specify /BINARY and do not include the /OUTPUT qualifier, an output file named AUDIT.AUDIT$JOURNAL is created.

The /BINARY, /BRIEF, and /FULL qualifiers cannot be used in combination.

EXAMPLES

1

```
$ ANALYZE/AUDIT /BINARY/EVENT_TYPE=LOGFAIL -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example writes all login failure audit messages from the current security audit log file to the binary file AUDIT.AUDIT$JOURNAL.

2

```
$ ANALYZE/AUDIT /BINARY/SINCE=TODAY/OUTPUT=25DEC89.AUDIT -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects all audit records generated today and writes the records in binary format to 25DEC89.AUDIT.

/BRIEF

Controls whether a brief (one line per record) format is used in ASCII displays.

FORMAT

/BRIEF *(default)*
/NOBRIEF

KEYWORDS

None.

DESCRIPTION

By default, records are displayed in the brief format. You must specify /FULL to have the full contents of each selected audit event record displayed.

The /BINARY, /BRIEF, and /FULL qualifiers cannot be used in combination.

EXAMPLE

```
$ ANALYZE/AUDIT /OUTPUT=AUDIT.LIS -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example produces an ASCII file in brief format by default. The file is written to AUDIT.LIS.

/EVENT_TYPE

Selects the classes of events to be extracted from the security log file. If you omit the qualifier or specify the ALL keyword, the event type is not used to select records.

FORMAT

/EVENT_TYPE=*(event-type[,...])*

KEYWORD

event type[,...]

Specifies the classes of events used to select records. You can specify any of the following event types:

Event Type	Meaning
[NO]ACCESS	Object access
[NO]ALL	All event types
[NO]AUDIT	Use of SET AUDIT command
[NO]BREAKIN	Breakin detection
[NO]INSTALL	Install operation
[NO]LOGFAIL	Unsuccessful login attempt
[NO]LOGIN	Successful login
[NO]LOGOUT	Successful logout
[NO]MOUNT	Execution of MOUNT or DISMOUNT command
[NO]NETUAF	Modification of the network proxy authorization file
[NO]RIGHTSDB	Modification of the rights database
[NO]SYSUAF	Modification of the system user authorization file

Specifying the negated form of an event class (for example, NOLOGFAIL) excludes the specified event class from the audit analysis report.

EXAMPLES

1

```
$ ANALYZE/AUDIT /EVENT_TYPE=LOGFAIL -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects records that match the event type LOGFAIL.

2

```
$ ANALYZE/AUDIT /EVENT_TYPE=(NOLOGIN,NOLOGOUT) -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example excludes all LOGIN and LOGOUT event class records from display.

/FULL

Controls whether a full format is used in ASCII displays. If you specify /NOFULL or omit the qualifier, records are displayed in the brief format.

FORMAT

/FULL
/NOFULL *(default)*

KEYWORDS

None.

DESCRIPTION

By default, records are displayed in the brief format. You must specify /FULL to have the full contents of each selected record displayed.

The /BINARY, /BRIEF, and /FULL qualifiers cannot be used in combination.

EXAMPLE

```
$ ANALYZE/AUDIT /FULL -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example displays the full contents of each selected record.

/IGNORE

Controls whether records matching the specified criteria are excluded.

FORMAT

/IGNORE=*criteria[,...]*

KEYWORD

criteria[,...]

Specifies that all records are selected except those matching any of the specified exclusion criteria. See the /SELECT qualifier description for a list of the possible criteria to use with the /IGNORE qualifier.

DESCRIPTION

Use the /IGNORE qualifier to exclude specific groups of audit records from the audit analysis report. When more than one keyword from the list of possible exclusion criteria are specified, records that meet any of the criteria are excluded.

EXAMPLE

```
$ ANALYZE/AUDIT /IGNORE=(SYSTEM=NAME=WIPER,USERNAME=MILANT) -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example excludes from the audit analysis report all records in the audit log file generated from node WIPER or from user MILANT (on any node).

/INTERACTIVE

Controls whether interactive command mode is enabled when the Audit Analysis Utility is invoked.

FORMAT

/INTERACTIVE *(default)*
/NOINTERACTIVE

KEYWORDS

None.

DESCRIPTION

Interactive command mode, enabled by default, allows you to interrupt the audit analysis report being displayed and issue commands that modify the criteria used to select or exclude records for the report.

To interrupt a full or brief audit analysis report and enter interactive mode commands, press CTRL/C. Enter commands at the *COMMAND>* prompt. Enter the CONTINUE command to leave interactive command mode and continue the audit analysis report or EXIT to terminate the session. See the command section for a complete description of each interactive mode command.

Specify /NOINTERACTIVE to disable interactive command mode.

Note: **Upon entering command mode, the current record is displayed in full format. The record may not match the selection or exclusion criteria specified in the previous ANALYZE/AUDIT command.**

EXAMPLES

1

```
$ ANALYZE/AUDIT /FULL -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example produces a full format display of the selected records. New records are displayed every three seconds. (See the /PAUSE qualifier description to find how to modify the duration of each record displayed.) Use the CTRL/C key combination to interrupt the display and enter interactive mode commands.

2

```
$ ANALYZE/AUDIT /FULL/NOINTERACTIVE -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example displays the first record selected and prompts you to press the RETURN key to display each additional selected record. Control returns to the DCL command level when all selected records have been displayed.

/OUTPUT

Specifies where to direct output from the Audit Analysis Utility. If you omit the qualifier, selected ASCII records are output to SYS$OUTPUT.

FORMAT

/OUTPUT*[=file-spec]*
/NOOUTPUT

KEYWORD

file-spec[,...]
Specifies the name of the file that is to contain the selected records. If you omit the device and directory specification, the current device and directory specification are used. If you omit the file name and type, the default file name AUDIT.LIS is used. If the output is binary (/BINARY) and you omit the /OUTPUT qualifier, the binary information is output to the file AUDIT.AUDIT$JOURNAL.

EXAMPLE

```
$ ANALYZE/AUDIT /BINARY/OUTPUT=BIN122588.DAT -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects audit records and outputs them in binary format to the file BIN122588.DAT.

/PAUSE

Specifies the length of time each record is displayed for full-format (/FULL) displays.

FORMAT

/PAUSE=*seconds*

KEYWORD

seconds

Specifies the duration (in seconds) of the full screen display. A value of 0 specifies that the system should not pause before displaying the next selected record. The default is 3 seconds.

DESCRIPTION

The /PAUSE qualifier can only be used with full-format (/FULL) displays to specify the length of time each record is displayed. By default, each record is displayed for a period of 3 seconds. A value of 0 results in a continuous display of audit records.

EXAMPLE

```
$ ANALYZE/AUDIT /FULL/PAUSE=1 -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example displays a selected record in full format every second. You can interrupt the display and enter interactive mode commands at any time by pressing CTRL/C. (See the Interactive Mode Command section for more information.)

/SELECT

Controls whether records matching the specified criteria are selected.

FORMAT

/SELECT=*(criteria[,...])*
/NOSELECT

KEYWORD

criteria[,...]

Specifies the criteria to be used to select records. If you omit the /SELECT qualifier, all event records are selected.

The possible criteria that can be specified are as follows:

ACCESS=(type,...)

Specifies the type of object access upon which the selection is based. It may be any of the following: READ, WRITE, EXECUTE, DELETE, or CONTROL.

ACCOUNT=(name,...)

Specifies the account name upon which selection is based. Full wildcarding of the account name is allowed.

DEVICE_NAME=(name,...)

Specifies the name of the device to be used in the selection of event records. Full wildcarding of the device name is allowed.

DISMOUNT_FLAGS=(name,...)

Specifies the names of the volume dismounting flags upon which selection is based. The available names are ABORT, CLUSTER, NOUNLOAD, and UNIT.

HOLDER=(list,...)

Specifies the characteristics of the identifier holder to be used in selecting event records.

Keyword	Description
NAME=name	Specifies the name of the holder. Full wildcarding of the name is allowed.
OWNER=value	Specifies the owner (UIC) of the holder.

IDENTIFIER=(attr,...)

Specifies that some attribute of an identifier should be used in selecting event records.

Keyword	Description
ATTRIBUTE=name	Specifies the name of the particular attribute. The available names are RESOURCE and DYNAMIC.
NAME=name	Specifies the original name of the identifier. Full wildcarding of the name is allowed.
NEW_NAME=name	Specifies the new name of the identifier. Full wildcarding is allowed.
VALUE=value	Specifies the original value of the identifier.
NEW_VALUE=value	Specifies the new value of the identifier.

IMAGE_NAME=(name,...)

Specifies the name of the image to be used when selecting event records. Full wildcarding of the image name is allowed.

INSTALL=(type,...)

Specifies the type of installation event to be considered when selecting event records.

Keyword	Description
FILE=name	Specifies the name of the installed file. Full wildcarding is allowed.
FLAGS=name	Specifies the names of the flags that correspond to the INSTALL qualifiers. (For example, OPEN corresponds to /OPEN.)
PRIVILEGES=name	Specifies the names of the privileges with which the file was installed.

LOCAL=(list,...)

Specifies the characteristics of the local (proxy) account to be used when selecting event records.

Keyword	Description
USERNAME=name	Specifies the name of the local account used. Full wildcarding of the name is allowed.

LOGICAL_NAME=(name,...)

Specifies the logical name of the volume mounted (or dismounted) upon which selection is based. Full wildcarding of the logical name is allowed.

MOUNT_FLAGS=(name,...)

Specifies the names of the volume mounting flags upon which selection is based. The available names are:

CACHE=(NONE,WRITETHROUGH)
CLUSTER
DATACHECK=(READ,WRITE)
FOREIGN
GROUP
INITIALIZATION=(ALLOCATE,CONTINUATION)

```
INTERCHANGE
MESSAGE
NOASSIST
NOAUTO
NODISKQ
NOHDR3
NOLABEL
NOWRITE
                         ⎧ ACCESSIBILITY      ⎫
                         ⎪ EXPIRATION         ⎪
OVERRIDE=(options[,...]) ⎨ IDENTIFICATION     ⎬
                         ⎪ SETID              ⎪
                         ⎪ LOCK               ⎪
                         ⎩ OWNER_IDENTIFIER   ⎭
SHARE
SYSTEM
```

OBJECT=(list,...)

Specifies which characteristics of an object should be used in selecting event records.

Keyword	Description
IDENTIFICATION=value	Specifies a unique object identification for the object (currently this is only the file identification (file ID) for a file).
NAME=name	Specifies the name of the object. Full wildcarding of the name is allowed.
OWNER=value	Specifies the owner (identifier value) of the object.
TYPE=name	Specifies the general object type. The available types are as follows: FILE SYSTEM_GLOBAL_SECTION GROUP_GLOBAL_SECTION

PARENT=(list,...)

Specifies which characteristics of the parent process (when a subprocess causes an event record to be generated) are used in selecting event records.

Keyword	Description
IDENTIFICATION=value	Specifies the process identification (PID) of the parent process.
NAME=name	Specifies the name of the parent process. Full wildcarding of the name is allowed.
OWNER=value	Specifies the owner (identifier value) of the parent process.
USERNAME=name	Specifies the user name of the parent process. Full wildcarding of the name is allowed.

PRIVILEGES_USED=(privs,...)

Specifies the privileges of the process to be used when selecting event records. Specify any of the following privileges: SYSPRV, BYPASS, GRPPRV, and READALL.

PROCESS=(list,...)

Specifies the characteristics of the process to be used when selecting event records.

Keyword	Description
IDENTIFICATION=value	Specifies the PID of the process.
NAME=name	Specifies the name of the process. Full wildcarding of the process name is allowed.

REMOTE=(list,...)

Specifies that some characteristic of the network request is to be used in selecting event records.

Keyword	Description
IDENTIFICATION=value	Specifies the DECnet address.
NODENAME=name	Specifies the DECnet node name. Full wildcarding of the node name is allowed.
USERNAME=name	Specifies the remote user name. Full wildcarding of the remote user name is allowed.

STATUS=type

Specifies the type of success status to be used in selecting event records.

Keyword	Description
SUCCESSFUL	Specifies a generic success class.
FAILURE	Specifies a generic failure class.
CODE=value	Specifies a specific completion status.

SYSTEM=(list,...)

Specifies the characteristics of the system to be used in selecting event records.

Keyword	Description
IDENTIFICATION=value	Specifies the numeric identification of the system.
NAME=name	Specifies the name of the system.

TERMINAL=(name,...)

Specifies the name of the terminal to be used when selecting event records. Full wildcarding of the terminal name is allowed.

USERNAME=(name,...)

Specifies the user name to be used when selecting event records. Full wildcarding of the user name is allowed.

VOLUME_NAME=(name,...)

Specifies that the name of the mounted (or dismounted) volume is to be used in selecting event records. Full wildcarding of the volume name is allowed.

EXAMPLES

1

```
$ ANALYZE/AUDIT /FULL/SELECT=USERNAME=JOHNSON -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects all records written to the security audit log file that were generated by user JOHNSON.

2

```
$ ANALYZE/AUDIT /FULL/SELECT=PRIVILEGES_USED=(SYSPRV,BYPASS) -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects all records written to the security audit log file that were generated by events through the use of either the SYSPRV or BYPASS privilege.

/SINCE

Controls whether records dated the same or later than the specified time are selected.

FORMAT

/SINCE*[=time]*
/NOSINCE

KEYWORD

time
Specifies the time used to select records. Records dated the same or later than the specified time are selected. You can specify an absolute time, delta time, or or a combination of the two. Observe the syntax rules for date and time described in the *VMS DCL Concepts Manual.*

If you specify /SINCE without the time, midnight of the current day is used.

EXAMPLES

1

```
$ ANALYZE/AUDIT /SINCE=25-JUL-1989 -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects records dated later than July 25, 1989.

2

```
$ ANALYZE/AUDIT /SINCE=25-JUL-1989:15:00 -
_$ SYS$MANAGER:SECURITY_AUDIT.AUDIT$JOURNAL
```

The command in this example selects records written after 3 P.M. on July 25, 1989.

/SUMMARY

Specifies that a summary of the selected records be produced after all records are processed.

You can use the /SUMMARY qualifier alone or in combination with the /BRIEF, /BINARY, or /FULL qualifier.

FORMAT

/SUMMARY
/NOSUMMARY

KEYWORDS

None.

EXAMPLES

1

```
$ ANALYZE/AUDIT /SUMMARY
```

The command in this example generates a summary report of all records processed, as shown in the following display:

```
Total records read:    10831             Records selected:       10831
Record buffer size:    512               Format buffer size:     128
Server messages:       0                 Customer messages:      0
Digital CSS messages:  0                 Layered prod messages:  0
Audit changes:         169               Installed db changes:   322
Login failures:        246               Breakin attempts:       0
Successful logins:     1719              Successful logouts:     951
System UAF changes:    33                Network UAF changes:    0
Rights db changes:     3                 Object accesses:        6976
Volume (dis)mounts:    412
```

2

```
$ ANALYZE/AUDIT/FULL/EVENT_TYPE=(BREAKIN,LOGFAIL) /SUMMARY
```

The command in this example generates a full-format listing of all logged audit messages that match the *breakin* or *log failure* event classes. A summary report is included at the end of the listing.

ANALYZE/AUDIT INTERACTIVE MODE COMMANDS

This section describes the interactive mode commands available with the Audit Analysis Utility. The qualifiers for this section follow the standard rules of DCL grammar.

To enter interactive mode commands, press CTRL/C at any time during the processing of a full or brief interactive display. At the *COMMAND>* prompt, you can enter additional interactive mode commands, the CONTINUE command to resume processing of the event records, or EXIT to terminate the session.

CONTINUE

Resumes processing of event records.

FORMAT CONTINUE

PARAMETERS

None.

QUALIFIERS

None.

EXAMPLE

```
COMMAND> DISPLAY/SINCE=25-JUN-1989/SELECT=USERNAME=POST
COMMAND> CONTINUE
```

The first command in this example selects only event records generated by user JOHNSON after June 25, 1989. The second command in the example displays a report based on the new selection criteria.

DISPLAY

Changes the criteria used to select event records. For a more complete description of any one of the following qualifiers, refer to the description of the same qualifier and its keywords in the preceding ANALYZE/AUDIT qualifier section.

FORMAT

DISPLAY

PARAMETERS

None.

QUALIFIERS

/BEFORE=time

Controls whether only those records dated earlier than the specified time are selected.

/BRIEF

Controls whether a brief (one line per record) format is used in ASCII displays.

/EVENT_TYPE=event-type[,...]

Controls whether only those records matching the specified event type are selected.

/FULL

Controls whether a full format for each record is used in ASCII displays.

/IGNORE=criteria[,...]

Controls whether records matching the specified criteria are excluded. If you specify /IGNORE two or more times, the criteria is combined. To specify a new set of exclusion criteria, include the /REMOVE qualifier with the /IGNORE qualifier.

/PAUSE=seconds

For full-format displays (/FULL), specifies the length of time each record is displayed.

/REMOVE

Controls whether the criteria specified by the /IGNORE and /SELECT qualifiers are no longer to be used to select event records to be displayed.

/SELECT=criteria[,...]

Controls whether only those records matching the specified criteria are selected. If you specify /SELECT two or more times, the criteria is combined. To specify a new set of selection criteria, include the /REMOVE qualifier with the /SELECT qualifier.

/SINCE[=time]

Controls whether only those records dated the same or later than the specified time are selected.

EXAMPLES

1

```
COMMAND> DISPLAY/EVENT_TYPE=SYSUAF
COMMAND> CONTINUE
```

The first command in this example selects records that were generated as a result of a modification to the system user authorization file (SYSUAF). The second command displays the selected records.

2

```
COMMAND> DISPLAY/SELECT=USERNAME=CRICK
COMMAND> CONTINUE







CTRL/C
COMMAND> DISPLAY/SELECT=USERNAME=WATSON
COMMAND> CONTINUE
```

The first DISPLAY command in this example selects records that were generated by user CRICK. The second command displays the selected records. The next DISPLAY command selects records that were generated by user WATSON. The last command in the example displays all records generated by users CRICK and WATSON.

EXIT

Terminates the session.

FORMAT

EXIT

PARAMETERS

None.

QUALIFIERS

None.

HELP

Provides online help information for using ANALYZE/AUDIT interactive mode commands.

FORMAT

HELP *[topic]*

PARAMETER

topic

Specifies the command for which help information is to be displayed. If you omit the keyword, HELP displays a list of available help topics, and prompts you for a particular keyword.

QUALIFIERS

None.

EXAMPLE

```
COMMAND> HELP DISPLAY
```

The command in this example displays help information about the interactive mode command DISPLAY.

LIST

Changes the criteria used to select event records. The LIST command is a synonym for DISPLAY. For a more complete description of any one of the following qualifiers, refer to the description of the same qualifier and its keywords in the preceding ANALYZE/AUDIT qualifier section.

FORMAT

LIST

PARAMETERS

None.

QUALIFIERS

/BEFORE=time

Controls whether only those records dated earlier than the specified time are selected.

/BRIEF

Controls whether a brief (one line per record) format is used in ASCII displays.

/EVENT_TYPE=event-type[,...]

Controls whether only those records matching the specified record type are selected.

/FULL

Controls whether a full format for each record is used in ASCII displays.

/IGNORE=criteria[,...]

Controls whether records matching the specified criteria are excluded. If you specify /IGNORE two or more times, the criteria is combined. To specify a new set of exclusion criteria, include the /REMOVE qualifier with the /IGNORE qualifier.

/PAUSE=seconds

For full-format displays (/FULL), specifies the duration for each record displayed.

/REMOVE

Controls whether the criteria specified by the /IGNORE and /SELECT qualifiers are no longer to be used to select event records to be displayed.

/SELECT=criteria[,...]

Controls whether only those records matching the specified criteria are selected. If you specify /SELECT two or more times, the criteria is combined. To specify a new set of exclusion criteria, include the /REMOVE qualifier with the /SELECT qualifier.

/SINCE[=time]

Controls whether only those records dated the same or later than the specified time are selected.

EXAMPLE

```
COMMAND> LIST/EVENT_TYPE=SYSUAF
COMMAND> CONTINUE
```

The first command in this example selects records that were generated as a result of a modification to the system user authorization file (SYSUAF). The second command displays the selected records.

NEXT FILE

Controls whether the current security audit log file is closed and the next log file opened. If there are no other audit log files to open, the audit analysis session is terminated and control returns to DCL.

FORMAT

NEXT FILE

PARAMETERS

None.

QUALIFIERS

None.

NEXT RECORD

Controls whether the next audit record is displayed. The NEXT RECORD command is synonymous with the command POSITION.

FORMAT

NEXT RECORD

PARAMETERS

None.

QUALIFIERS

None.

POSITION

Moves the full-format display forward or backward the specified number of event records.

FORMAT

POSITION *number*

PARAMETER

number

For positive numbers, displays the record that is the specified number of records after the current record. For negative numbers, displays the record that is the specified number of records before the current record.

QUALIFIERS

None.

EXAMPLES

1

```
COMMAND> POSITION 100
```

The command in this example moves the display forward 100 event records.

2

```
COMMAND> POSITION -100
```

The command in this example moves the display back 100 event records.

SHOW

Displays information about selection or exclusion criteria currently being used to select event records.

FORMAT

SHOW *option[,...]*

PARAMETER

option[,...]

Displays information about selection or exclusion criteria currently being used to select records. Specify one or more of the following options:

Option	Meaning
ALL	Displays all criteria being used to select event records.
EXCLUSION_CRITERIA	Displays the criteria being used to exclude event records.
SELECTION_CRITERIA	Displays the criteria being used to select event records.

QUALIFIERS

None.

EXAMPLE

```
COMMAND> SHOW SELECTION_CRITERIA
```

The command in this example displays the selection criteria currently in use to select records.

A Security Audit Message Format

This appendix describes the format of the auditing messages written to the security auditing log file (SECURITY_AUDIT.AUDIT$JOURNAL in the SYS$COMMON:[SYSMGR], by default). Each security audit record consists of a header packet followed by one or more data packets. The number of data packets depends on the type of information being sent. The remainder of this appendix describes the format of the audit header and data packets.

A.1 Audit Header Packet

Figure A–1 illustrates the format of the audit header packet; Table A–1 describes the fields contained in this packet.

Figure A–1 Audit Header Packet Format

<table>
<tr><td colspan="2">NSA$W_RECORD_SUBTYPE</td><td>NSA$W_RECORD_TYPE</td></tr>
<tr><td colspan="2">NSA$W_PACKET_COUNT</td><td>NSA$W_FLAGS</td></tr>
<tr><td>NSA$B_VERSION</td><td>unused</td><td>unused</td></tr>
<tr><td colspan="2">unused</td><td>unused</td></tr>
<tr><td colspan="2">NSA$W_FACILITY</td><td>unused</td></tr>
</table>

ZK–0825A–GE

Table A–1 Audit Header Packet

Field	Symbolic Offset	Contents
type	NSA$W_RECORD_TYPE	Indicates the type of event that has occurred, as described in Table A–2.
subtype	NSA$W_RECORD_SUBTYPE	Further defines the type of event that has occurred, as described in Table A–3.
flags	NSA$W_FLAGS	Identifies any flags associated with the audited event. Reserved for future use. (word)
packet count	NSA$W_PACKET_COUNT	Number of data packets in the audit record. (word)
record size	NSA$W_REC_SIZE	Total size of audit message (header packet plus all data packets). (word)
version	NSA$B_VERSION	Indicates the version of the security auditing facility. The symbol NSA$C_VERSION_2 indicates the current version. (byte)
facility	NSA$W_FACILITY	The facility code for the generated event. By default, this field is zero, indicating a VMS generated event. (word)

Table A–2 lists the symbols that represent the type of security event that has occurred.

Table A–2 NSA$W_RECORD_TYPE Event Types

Symbol	Meaning
NSA$C_MSG_ACCESS	Object access attempted
NSA$C_MSG_AUDIT	SET AUDIT command issued
NSA$C_MSG_BREAKIN	Breakin attempt detected
NSA$C_MSG_INSTALL	Install Utility used to install a file
NSA$C_MSG_LOGFAIL	Login failure
NSA$C_MSG_LOGIN	Successful login
NSA$C_MSG_LOGOUT	Successful logout
NSA$C_MSG_MOUNT	Device mount or dismount
NSA$C_MSG_NETUAF	Modification to network proxy database
NSA$C_MSG_RIGHTSDB	Modification to rights database
NSA$C_MSG_SYSUAF	Modification to system authorization database

For each audit event record type defined by NSA$W_RECORD_TYPE, there is a record subtype defined by the symbol NSA$W_RECORD_SUBTYPE, which further defines the event. Table A–3 describes those symbols that represent the record subtypes.

Table A–3 Audit Record Subtypes

Symbol	Meaning
Subtypes for NSA$C_MSG_ACCESS Record Type	
NSA$C_FILE_ACCESS	File access attempted
NSA$C_GRPGBL_ACCESS	Group global section access attempted
NSA$C_SYSGBL_ACCESS	System global section access attempted
Subtypes for NSA$C_MSG_AUDIT Record Type	
NSA$C_AUDIT_TERMINATE	Audit server shutdown (SET AUDIT/SERVER=EXIT)
NSA$C_AUDIT_INITIATE	Audit server startup (SET AUDIT/SERVER=START)
Subtypes for NSA$C_MSG_BREAKIN, NSA$C_MSG_LOGFAIL, NSA$C_MSG_LOGIN, and NSA$C_MSG_LOGOUT Record Types	
NSA$C_BATCH	Batch process breakin, login, logout, or login failure attempt
NSA$C_DETACHED	Detached process breakin, login, logout, or login failure attempt
NSA$C_DIALUP	Dialup interactive breakin, login, logout, or login failure attempt
NSA$C_LOCAL	Local interactive breakin, login, logout, or login failure attempt
NSA$C_NETWORK	Network server task breakin, login, logout, or login failure attempt
NSA$C_REMOTE	Interactive breakin, login, logout, or login failure attempt from another network node
NSA$C_SUBPROCESS	Subprocess breakin, login, logout, or login failure attempt
Subtypes for NSA$C_MSG_INSTALL Record Type	
NSA$C_INSTALL_ADD	Known image installed
NSA$C_INSTALL_REMOVE	Known image deleted

(continued on next page)

Table A–3 (Cont.) Audit Record Subtypes

Symbol	Meaning
Subtypes for NSA$C_MSG_MOUNT Record Type	
NSA$C_VOL_DISMOUNT	Volume dismount
NSA$C_VOL_MOUNT	Volume mount
Subtypes for NSA$C_MSG_NETUAF Record Type	
NSA$C_NETUAF_ADD	Record added to network proxy authorization file
NSA$C_NETUAF_DELETE	Record removed from network proxy authorization file
NSA$C_NETUAF_MODIFY	Record modified in network proxy authorization file
Subtypes for NSA$C_MSG_RIGHTSDB Record Type	
NSA$C_RDB_ADD_ID	Identifier added to rights database
NSA$C_RDB_CREATE	Rights database created
NSA$C_RDB_GRANT_ID	Identifier granted to holder
NSA$C_RDB_MOD_HOLDER	Identifier holder list modified
NSA$C_RDB_MOD_ID	Identifier name or attributes modified
NSA$C_RDB_REM_ID	Identifier removed from rights database
NSA$C_RDB_REVOKE_ID	Identifier deleted from holder's process rights list
Subtypes for NSA$C_MSG_SYSUAF Record Type	
NSA$C_SYSUAF_ADD	Record added to system authorization file
NSA$C_SYSUAF_COPY	Record copied in system authorization file
NSA$C_SYSUAF_DELETE	Record deleted from system authorization file
NSA$C_SYSUAF_MODIFY	Record modified in system authorization file
NSA$C_SYSUAF_RENAME	Record renamed in system authorization file

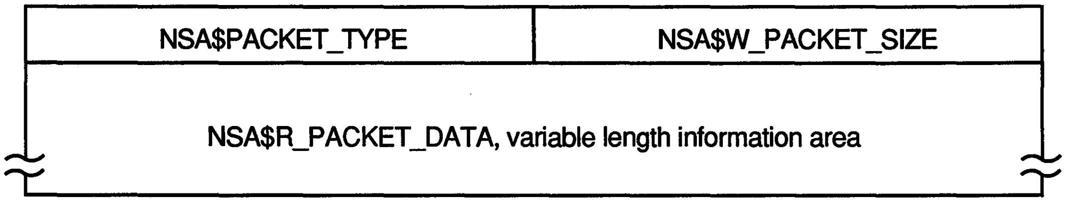
In addition, the symbol NSA$R_PACKET_LIST is defined as a pointer to the beginning of the first audit data packet.

A.2 Audit Data Packets

Figure A–2 illustrates the format of an audit data packet; Table A–4 describes the fields contained in these packets.

Note that audit data packets do not appear in any predefined order within an event message. Packet types may appear more than once throughout the event message.

Figure A–2 Audit Data Packet Format



ZK–0809A–GE

Table A–4 Audit Data Packet

Field	Symbolic Offset	Contents
Packet size	NSA$W_PACKET_SIZE	Indicates the size of the data packet. (word)
Packet type	NSA$W_PACKET_TYPE	Indicates the type of data in the packet, as described in Table A–5.
Packet data	NSA$R_PACKET_DATA	Variable length field containing the packet data.

Table A–5 identifies the type of data in the audit data packet.

Table A–5 NSA$W_PACKET_TYPE Data Types

Symbol	Meaning
NSA$C_PKT_ACCESS_DESIRED	The data in the packet contains the access requested/granted to the object. (Longword)
NSA$C_PKT_ACCOUNT	The data in the packet contains the account name associated with the process causing the auditable event. (ASCII string)
NSA$C_PKT_ALARM_DISABLE	The data in the packet specifies the security events to disable. (Vector)
NSA$C_PKT_ALARM_ENABLE	The data in the packet specifies the security events to enable. (Vector)

(continued on next page)

Table A–5 (Cont.) NSA$W_PACKET_TYPE Data Types

Symbol	Meaning
NSA$C_PKT_ALARM_NAME	The data in the packet contains the name of the user (or the security class operators terminal) to which the record will be directed. (ASCII string)
NSA$C_PKT_APPL_DATA	The data in the packet contains arbitrary application data. (Vector)
NSA$C_PKT_AUDIT_NAME	The data in the packet contains the name of the journal to which the record will be directed. (ASCII string)
NSA$C_PKT_DEFAULT_USERNAME	The data in the packet contains the default local user name to use for incoming network proxy requests. (ASCII string)
NSA$C_PKT_DEVICE_NAME	The data in the packet contains the device name on which the volume resides. (ASCII string)
NSA$C_PKT_DISMOUNT_FLAGS	The data in the packet contains the dismount flags. (Longword)
NSA$C_PKT_FIELD_NAME	The data in the packet contains the name of the field being modified. This is used in combination with NSA$C_PKT_ORIGINAL_DATA and NSA$C_PKT_NEW_DATA. (ASCII string)
NSA$C_PKT_FINAL_STATUS	The data in the packet contains the status (error or success) which caused the auditing facility to be invoked. (Longword)
NSA$C_PKT_HOLDER_NAME	The data in the packet contains the ID holder username. (ASCII string)
NSA$C_PKT_HOLDER_OWNER	The data in the packet contains the owner ID for the identifier. (Longword)
NSA$C_PKT_ID_ATTRIBUTES	The data in the packet contains the new attributes of the identifier. (Longword)
NSA$C_PKT_ID_NAME	The data in the packet contains the name of the identifier. (ASCII string)
NSA$C_PKT_ID_NEW_NAME	The data in the packet contains the new name of the identifier. (ASCII string)
NSA$C_PKT_ID_NEW_VALUE	The data in the packet contains the new value of the identifier. (Longword)
NSA$C_PKT_ID_VALUE	The data in the packet contains the value of the identifier. (Longword)
NSA$C_PKT_IDENTIFIERS_USED	The data in the packet contains any identifiers used (from the ACE granting access) to gain access to the object. (Longword vector)

(continued on next page)

Table A–5 (Cont.) NSA$W_PACKET_TYPE Data Types

Symbol	Meaning
NSA$C_PKT_IMAGE_NAME	The data in the packet contains the name of the image being executed at the time the event took place. (ASCII string)
NSA$C_PKT_INSTALL_FILE	The data in the packet contains the name of the installed file. (ASCII string)
NSA$C_PKT_INSTALL_FLAGS	The data in the packet contains the flags associated with the installed file. (Longword)
NSA$C_PKT_INSTALL_PRIVS	The data in the packet contains the privileges associated with the installed file. (Quadword)
NSA$C_PKT_LISTENER_DEVICE	The data in the packet contains the name of the mailbox device to which a copy of the event message will be sent. (ASCII string)
NSA$C_PKT_LOCAL_USERNAME	The data in the packet contains the user names of the accounts that may be used for incoming network proxy requests. (ASCII string)
NSA$C_PKT_LOGICAL_NAME	The data in the packet contains the logical name associated with the device. (ASCII string)
NSA$C_PKT_MOUNT_FLAGS	The data in the packet contains the mount flags. (Longword)
NSA$C_PKT_NEW_DATA	The data in the packet contains the value to be utilized after the event occurs. (Vector)
NSA$C_PKT_OBJECT_ID	The data in the packet contains a unique object identification code. Currently this only applies to files, and is the file identification (file ID). (Longword vector)
NSA$C_PKT_OBJECT_NAME	The data in the packet contains the object's name. (ASCII string)
NSA$C_PKT_OBJECT_OWNER	The data in the packet contains the owner identifier (UIC) of the process causing the auditable event. (Longword)
NSA$C_PKT_OBJECT_PROTECTION	The data in the packet contains the UIC based protection of the object. (Word or Longword Vector)
NSA$C_PKT_OBJECT_TYPE	The data in the packet contains the object's type code (see $ACLDEF). (Longword)
NSA$C_PKT_ORIGINAL_DATA	The data in the packet contains the value prior to the event taking place. (Vector)
NSA$C_PKT_PARENT_ID	The data in the packet contains the process identification (PID) of the parent process. (This is only used when auditing events pertaining to a subprocess.) (Longword)

(continued on next page)

Table A–5 (Cont.) NSA$W_PACKET_TYPE Data Types

Symbol	Meaning
NSA$C_PKT_PARENT_NAME	The data in the packet contains the parent process name. (This is only used when auditing events pertaining to a subprocess.) (ASCII string)
NSA$C_PKT_PARENT_OWNER	The data in the packet contains the owner identifier (UIC) of the parent process. (Longword)
NSA$C_PKT_PARENT_USERNAME	The data in the packet contains the user name associated with the parent process. (ASCII string)
NSA$C_PKT_PASSWORD	The data in the packet contains the failing password for break-in attempts. (ASCII string)
NSA$C_PKT_PERFORMANCE_NOP	This packet contains no useful information. This packet code is used when there is a performance advantage to be gained from building a static packet list, and then removing those packets that do not apply to the current event.
NSA$C_PKT_PRIVS_USED	The data in the packet contains any privileges used to gain access to the object. (Longword)
NSA$C_PKT_PROCESS_ID	The data in the packet contains the PID of the process that caused the auditable event. (Longword)
NSA$C_PKT_PROCESS_NAME	The data in the packet contains the process name for the process causing the auditable event. (ASCII string)
NSA$C_PKT_REMOTE_NODE_ID	The data in the packet contains the DECnet address of the remote process. (Longword)
NSA$C_PKT_REMOTE_NODENAME	The data in the packet contains the DECnet node name of the remote process. (ASCII string)
NSA$C_PKT_REMOTE_USERNAME	The data in the packet contains the user name of the remote process. (ASCII string)
NSA$C_PKT_REPLY_MAILBOX	The data in the packet contains the name of a mailbox to which the event completion status will be written. (ASCII string)
NSA$C_PKT_SUBJECT_CLASS	The data in the packet contains the current access class of the process causing the auditable event. (Longword vector)
NSA$C_PKT_SUBJECT_OWNER	The data in the packet contains the owner identifier (UIC) of the process causing the event. (Longword)

(continued on next page)

Table A–5 (Cont.) NSA$W_PACKET_TYPE Data Types

Symbol	Meaning
NSA$C_PKT_SYSTEM_NAME	The data in the packet contains the SCS name of the node on which the event took place (SYSGEN parameter SCSNODE). (ASCII string)
NSA$C_PKT_SYSTEM_ID	The data in the packet contains the SCS identification of the cluster node on which the event took place (SYSGEN parameter SCSSYSTEMID). (Longword)
NSA$C_PKT_TERMINAL	The data in the packet contains the name of the terminal to which the process was connected at the time of the auditable event. (ASCII string)
NSA$C_PKT_TIME_STAMP	The data in the packet contains the time that the event occurred. (Quadword)
NSA$C_PKT_UAF_ADD	The data in the packet contains the name of the authorization record being added. (ASCII string)
NSA$C_PKT_UAF_COPY	The data in the packet contains the original and new names of the authorization record being copied.
NSA$C_PKT_UAF_DELETE	The data in the packet contains the name of the authorization record being removed. (ASCII string)
NSA$C_PKT_UAF_FIELDS	The data in the packet contains the codes indicating the fields being changed in an authorization record (along with the new value).
NSA$C_PKT_UAF_MODIFY	The data in the packet contains the name of the authorization record being modified. (ASCII string)
NSA$C_PKT_UAF_RENAME	The data in the packet contains the name of the authorization record being renamed. (ASCII string)
NSA$C_PKT_UAF_SOURCE	The data in the packet contains the user name of the source record used for a copy operation. (ASCII string)
NSA$C_PKT_USERNAME	The data in the packet contains the user name associated with the process causing the auditable event. (ASCII string)
NSA$C_PKT_VOLUME_NAME	The data in the packet contains the volume name. (ASCII string)
NSA$C_PKT_VOLUME_SET_NAME	The data in the packet contains the volume set name. (ASCII string)

Index

How to Order Additional Documentation

Technical Support

If you need help deciding which documentation best meets your needs, call 800-343-4040 before placing your electronic, telephone, or direct mail order.

Electronic Orders

To place an order at the Electronic Store, dial 800-DEC-DEMO (800-332-3366) using a 1200- or 2400-baud modem. If you need assistance using the Electronic Store, call 800-DIGITAL (800-344-4825).

Telephone and Direct Mail Orders

Your Location	Call	Contact
Continental USA, Alaska, or Hawaii	800-DIGITAL	Digital Equipment Corporation P.O. Box CS2008 Nashua, New Hampshire 03061
Puerto Rico	809-754-7575	Local DIGITAL subsidiary
Canada	800-267-6215	Digital Equipment of Canada Attn: DECdirect Operations KAO2/2 P.O. Box 13000 100 Herzberg Road Kanata, Ontario, Canada K2K 2A6
International	————	Local DIGITAL subsidiary or approved distributor
Internal[1]	————	SDC Order Processing - WMO/E15 *or* Software Distribution Center Digital Equipment Corporation Westminster, Massachusetts 01473

[1] For internal orders, you must submit an Internal Software Order Form (EN-01740-07).

Reader's Comments

VMS Audit Analysis Utility Manual
AA–NG63A–TE

Please use this postage-paid form to comment on this manual. If you require a written reply to a software problem and are eligible to receive one under Software Performance Report (SPR) service, submit your comments on an SPR form.

Thank you for your assistance.

I rate this manual's:	Excellent	Good	Fair	Poor
Accuracy (software works as manual says)	□	□	□	□
Completeness (enough information)	□	□	□	□
Clarity (easy to understand)	□	□	□	□
Organization (structure of subject matter)	□	□	□	□
Figures (useful)	□	□	□	□
Examples (useful)	□	□	□	□
Index (ability to find topic)	□	□	□	□
Page layout (easy to find information)	□	□	□	□

I would like to see more/less ______

What I like best about this manual is ______

What I like least about this manual is ______

I found the following errors in this manual:

Page   Description

Additional comments or suggestions to improve this manual:

I am using **Version** ______ of the software this manual describes.

Name/Title ______ Dept. ______
Company ______ Date ______
Mailing Address ______
______ Phone ______

- Do Not Tear - Fold Here and Tape

digital™

No Postage
Necessary
if Mailed
in the
United States

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

DIGITAL EQUIPMENT CORPORATION
Corporate User Publications—Spit Brook
ZK01-3/J35 110 SPIT BROOK ROAD
NASHUA, NH 03062-9987

- Do Not Tear - Fold Here

Cut Along Dotted Line

Reader's Comments

VMS Audit Analysis Utility Manual
AA–NG63A–TE

Please use this postage-paid form to comment on this manual. If you require a written reply to a software problem and are eligible to receive one under Software Performance Report (SPR) service, submit your comments on an SPR form.

Thank you for your assistance.

I rate this manual's:	Excellent	Good	Fair	Poor
Accuracy (software works as manual says)	□	□	□	□
Completeness (enough information)	□	□	□	□
Clarity (easy to understand)	□	□	□	□
Organization (structure of subject matter)	□	□	□	□
Figures (useful)	□	□	□	□
Examples (useful)	□	□	□	□
Index (ability to find topic)	□	□	□	□
Page layout (easy to find information)	□	□	□	□

I would like to see more/less ______________________________

____

____

What I like best about this manual is ______________________________

____

____

What I like least about this manual is ______________________________

____

____

I found the following errors in this manual:

Page Description

______ ______________________________

______ ______________________________

______ ______________________________

______ ______________________________

______ ______________________________

Additional comments or suggestions to improve this manual:

____

____

____

____

I am using **Version** ______ of the software this manual describes.

Name/Title ______________________________ Dept. ______________
Company ______________________________ Date ______________
Mailing Address ______________________________
______________________________ Phone ______________

– Do Not Tear - Fold Here and Tape

digital™

No Postage
Necessary
if Mailed
in the
United States

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 33 MAYNARD MASS.

POSTAGE WILL BE PAID BY ADDRESSEE

DIGITAL EQUIPMENT CORPORATION
Corporate User Publications—Spit Brook
ZK01–3/J35 110 SPIT BROOK ROAD
NASHUA, NH 03062-9987

- Do Not Tear - Fold Here

Cut Along Dotted Line