NRS AUDIT SME

Document Number NAS-0023-4

North Ridge Software, Inc.

June 2006

Copyright Notice

North Ridge Software, Inc.
1305 11th Street
Bellingham, Washington 98225
(360) 676-5999

FAX (360) 733-5970

Disclaimer

Acknowledgements

References within this manual to the following products should be recognized as references to proprietary products and trademarks of the following firms:

CCA MODEL204

CA ACF2, IDMS, ROSCOE, and TOPSECRET

IBM ACF/VTAM, ACF/TCAM, NMPF, NPDA, VM/GCS, OS/VS1, NETVIEW, NLDM, NPA, CMS, MVS, MVS/XA, MVS/ESA, DOS/VSE, CICS/VS, TSO, IMS, RACF, NPDA, and NCCF

Table of Contents

List of Illustrations

Introduction

The **NRS Audit SME** is available as "shareware" from North Ridge Software, Inc. to assist VM and MVS installations in improving understanding about the network related activities that a specific VTAM domain is involved with.

The Audit SME uses the Secondary Authorization function within the VTAM Session Management Exit (ISTEXCAA) to:

1. identify the specific sessions being established within the VTAM domain
2. summarize the number of sessions a given domain is involved with
3. identify the specific Subareas and SNA Networks that a single domain has contact with during VTAM execution

This Audit SME has been tested with ACF/VTAM Release 3.1.1, 3.2, 3.3, and 3.4. It makes use only of documented facilities that exist within the Session Management Exit's interface to ACF/VTAM and should operate correctly on subsequent versions of ACF/VTAM. If you experience problems, etc. in getting it to operate, please send your comments along to the Audit SME Author at NRS.

The Goal

The intent of the Audit SME is to enable interested installations in the collection of information associated with the network processing of a VTAM domain. The Audit SME is intended to provide you with an improved confidence that you either do (or do not) have adequate controls in place to control your VTAM Domain(s).

NRS is also hopeful that you will be interested in controlling which sessions and activities can occur in your host. The Network Center's **Access** component is a fully implemented and supported Session Management Exit capable of enforcing a set of rules established for your domain. If you'd like more information about Access, just give us a call. We'd be happy to answer any questions you may have (about Access or the Audit SME).

Licensing

The NRS Audit SME is proprietary to NRS, but you are granted permission to use it on any computer system you would like at no charge. You are also authorized to reproduce it and pass it along to another installation, provided you retain the NRS Copyright and related identifying marks.

If you do replicate the Audit SME, you may **not** charge the recipient in any manner (direct or indirect) for the NRS Audit SME (except a shipping and handling fee that does not exceed $15.00 U.S.).

North Ridge Software

North Ridge Software is an independently owned Washington State corporation involved with the development, marketing, sales, and support of a variety of VTAM based software products.

The Audit SME was originally developed in response to multiple requests received after session presentations at various national and international conferences associated with security and auditing concerns. The Audit SME has served multiple purposes during its existence and will continue to evolve. If you have any suggestions, comments, etc. you can forward them to:

```
Audit SME Author
North Ridge Software
1305 11th Street #302
Bellingham, Washington 98225

Phone:   (360) 676-5999
FAX:     (360) 733-5970
```

Figure 1. Audit SME Author Address

We do not guarantee that you'll receive an answer, but we will seriously consider any suggestions for incorporation in subsequent versions of the Audit SME.

If you would like to be included on a mailing list for notification of an updated Audit SME, send your name and address to the address listed above.

Access

Access is the name of The Network Center's component (software product) that provides full control over session approval via the Session Management Exit. In addition to monitoring and controlling the session activity, you can also:

1. dynamically configure all "rules" of access
2. interactively monitor the Session Management Exit operation during execution
3. get someone else (NRS) to support your Session Management Exit
4. utilize CUA based panels in TSO or CMS to administer the Session Management Exit
5. produce accounting records (OS SMF, VM Account) describing desired events
6. interrogate the contents of the VTAM address space via the Query facility of The Network Center

Contact the NRS offices for additional information about **Access**.

Custom Exits

The Audit SME source code is not included on the distribution tape to eliminate support problems associated with distributing "free" software. The Audit SME can be configured via the IBM SuperZap utility to select functions, which eliminates the variations that might be introduced by local changes to the source.

However, NRS does make available custom exits (source code included) under a variety of contractual arrangements with individual clients. If you are interested in acquiring a custom Session Management Exit with or without ongoing support, please contact the NRS *Custom Services* division for a quotation.

Distributed OS Dataset Members

After you have unloaded the distribution datasets, you will find the following members in the NRS.NAS.DATA library:

COPYRITE a copyright and limited license statement

NASFAX a sample FAX form you can use to provide feedback to the Audit SME Author

NAS1403N the formatted output of NAS0023 generally suitable for printing on a 1403 type printer

NASOPTS SuperZap input stream to set the Audit SME's options

NASZAP Sample JCL to execute the SuperZap service aid to select the Audit SME options

NAS0023 DCF (Document Composition Facility) input that is the source for this manual

The NRS.NAS.LOAD library contains a single member:

ISTEXCAA the executable Audit SME

Distributed VM Files

The following files will be reloaded to the CMS mini-disk when you VMFPLC2 LOAD the tape:

COPYRITE MEMO a copyright and limited license statement

NASFAX MEMO a sample FAX form you can use to provide feedback to the Audit SME Author

NAS0023 1403N6 the formatted output of NAS0023 generally suitable for printing on a 1403 type printer on 8.5" x 11" paper (6 lines per inch)

NAS0023 LIST3820 the formatted output of NAS0023 that can be printed on an available page type printer (3812, 3820, 3800, etc.)

NASOPTS ZAP SuperZap input stream to set the Audit SME's options

NASZAP EXEC Sample EXEC to execute the SuperZap service aid to select the Audit SME options

NAS0023 SCRIPT DCF (Document Composition Facility) input that is the source for this manual

Installation

The installation of the NRS Audit SME consists of 4 basic steps:

1. Unload the distribution tape or upload the distribution files from the diskette
2. Customize NASOPTS for your purposes
3. Modify the VTAM JCL or EXEC
4. Restart VTAM

Unload the Distribution Tape

Unloading the distribution files from the tape differs by operating system. Follow the instructions below, as appropriate for your environment.[1]

Distribution Tape Format

The distribution tape contains the necessary files for both OS and VM installations. It is in the general form:

File	Used by	Contents	Format	Space Requirements
1	OS	NRS.NAS.DATA	PO	1 Cylinder 3380
2	OS	NRS.NAS.LOAD	PO	1 Cylinder 3380
3	VM	VM distribution files	VMFPLC2	1000 1K CMS blocks

Figure 2. Distribution Tape Format

The tape has the general form of a standard labeled OS tape with a VOLSER equal to NASnnn, where:

NAS is a 3 letter constant representing the NRS Audit SME

nnn is a 3 digit "version" identifier that establishes the precise release of the Audit SME on the tape (the VOLSER can also be found on the external tape label)

---

[1] If you are installing from a diskette instead of a 3420/3480 tape, simply review the README.TXT file for appropriate instructions. You should then resume this installation from "Customization" on page 7.

OS

You can unload the distribution tape in OS systems by executing IEBCOPY to restore the first two tape datasets to disk. An example IEBCOPY job stream follows:[2]

```
//jobname JOB (accounting information),'NRS SME',
//            CLASS=a,MSGCLASS=*
//*
//NASDATA  EXEC PGM=IEBCOPY
//SYSPRINT DD  SYSOUT=*
//SYSUT1   DD  DSN=NRS.NAS.DATA,DISP=(OLD,PASS),
//             UNIT=tape,VOL=SER=NASnnn,
//             LABEL=(1,SL,EXPDT=98000)
//SYSUT2   DD  DSN=nrs.NAS.DATA,DISP=(,CATLG,DELETE),
//             UNIT=sysda,SPACE=(CYL,(1,1,20))
//SYSUT3   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT4   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//*
//NASLOAD  EXEC PGM=IEBCOPY
//SYSPRINT DD  SYSOUT=*
//SYSUT1   DD  DSN=NRS.NAS.LOAD,DISP=OLD,
//             UNIT=tape,VOL=SER=NASnnn,
//             LABEL=(2,SL,EXPDT=98000)
//SYSUT2   DD  DSN=nrs.NAS.LOAD,DISP=(,CATLG,DELETE),
//             UNIT=sysda,SPACE=(CYL,(1,1,20))
//SYSUT3   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//SYSUT4   DD  UNIT=SYSDA,SPACE=(CYL,(1,1))
//*
```

Figure 3. OS Unload JCL

VM

Installation in VM consists of simply reloading the contents of the distribution file 3 to a suitable CMS mini-disk. After allocating and formatting a CMS mini-disk of at least 1,000 1K blocks, accessing it as the A disk, then issue the following commands:

```
        TAPE FSF 7
        VMFPLC2 LOAD  (18TRACK)
```

Figure 4. VM Unload Commands

Note: You should use the 18TRACK option only if you are unloading from a 3480 (cartridge) type media.

---

[2] You should review the sample JCL and fill in any lower case information with values appropriate to your installation).

Customization

The Audit SME is distributed with the most common values already set in place. We encourage you to **use it unchanged** from the tape before you begin customizing it. The Audit SME will display a single message on the console for each unique SSCP and network it encounters and summary statistics about the number of sessions at approximately one hour intervals.

An example of this output is (blank lines have been added to simplify the example and are not actually produced by the Audit SME):

```
NRSFE01 The NRS Audit SME Version 1.0.2, Copyright (c) 1993
NRSFE02   North Ridge Software, Inc.
NRSFE03   1305 11th Street
NRSFE04   Bellingham, Washington 98225
NRSFE05   (360) 676-5999 FAX (360) 733-5970
NRSFE06   IBMMail Exchange US3NN001 IIN NRSI001
NRSFE12 You can obtain a complete SME from NRS called Access, which is a
NRSFE13   portion of The Network Center. Call NRS at (360) 676-5999!
NRSFE14 ISTEXCAA base is 00269008 and SME is at 002CE000
NRSFE10 VM VTAM=VV34 Netid=NRS SSCP=SSCP34 HOSTPU=VTAM34 Address= 34

NRS0106 New node recognized, Network=NRS Sscp=SSCP34 Subarea= 34

NRS0106 New node recognized, Network=NRS Sscp=SSCP1 Subarea= 1

NRS0108 Total sessions since 92.226 at 15:39:15= 3, 92.226 at 15:39:15= 3
NRS0110   NRS SSCP34 = 5 Plu= 3 Slu= 2 Interval= 5
NRS0110   NRS SSCP1 = 1 Plu= 0 Slu= 1 Interval= 1
```

Figure 5. Sample Default Execution Output

The first group of messages is issued the first time that the Audit SME receives control. A NRS0106 message is issued each time a new Netid and SSCP combination is encountered. The NRS0108 and NRS0110 messages are issued approximately once an hour summarizing the number of sessions and half sessions that have involved the specific Netid and SSCP.[3]

The PUT option produces a copy of these messages into the NASLOG definition (SYSOUT file or PRINTER) that includes the julian date and time of day as a message prefix. This prefix will allow you to measure the real interval between INTERVAL reporting and compute "session rates", etc.

---

[3] The Audit SME allocates sufficient room (virtual storage) to accumulate information for 1,000 unique combinations of Netid and SSCP.

You may wish to change the Audit SME's operational characteristics prior to completing installation. Reference "Operation" on page 11 for details on what the various options are to control the Audit SME's output results.

Options are set within the Audit SME by modifying the executable code (load module) via an operating system utility identified as **SuperZap**. There are sample files on the distribution tape to aid you in utilizing this IBM provided utility.

Consult the following member or file for an example of the execution requirements for the SuperZap utility:

Member/File	***Contents***
NASZAP	this member in the OS DATA library contains sample JCL to execute the SuperZap utility or "Service Aid"
NASZAP EXEC	this CMS file contains the sample CMS commands necessary to run the ZAP maintenance command
NASOPTS	this member or file (file type of ZAP in CMS) contains the offsets and VER/REP statements required to set one or more options in the Audit SME. An example of this file is listed in "Appendix B. NRS Audit SME Options Member/File" on page 21.

Modify VTAM JCL or EXEC

To activate the Audit SME, you will need to make the OS LOAD library or VM LOADLIB available to VTAM.

OS

OS installations should place the NRS.NAS.LOAD library in the concatenation sequence on the VTAM VTAMLIB DD statement. You can also move the single routine identified as ISTEXCAA to a suitable VTAMLIB library. The Audit SME **does not require** APF authorization to execute.

```
//NET      EXEC PGM=vtam,REGION=nnnnn
//STEPLIB  DD  DSN=SYS1.VTAMOBJ,DISP=SHR
//VTAMLST  DD  DSN=SYS1.VTAMLST,DISP=SHR
//VTAMLIB  DD  DSN=SYS1.VTAMLIB,DISP=SHR
//         DD  DSN=NRS.NAS.LOAD,DISP=SHR     <=====
//NASLOG   DD  SYSOUT=A                      <=====
      .
      .
      .
```

The NASLOG DD statement is **not required** unless you activate the Audit SME's PUT option (see "PUT" on page 15). If active, the NASLOG output can also be routed to a disk dataset, but make sure it is large enough to hold the output generated by the Audit SME.

VM

VM installations will have to add the NASEXCAA LOADLIB to the GLOBAL LOADLIB command issued when VTAM initializes in the GCS virtual machine. The following example is extracted from a typical VMVTAM GCS initialization EXEC:

```
/**
*** VTAM initialization
**/
        .
        .
        .
   'ACC 29A F/F'
   'FILEDEF NASLOG PRINTER'
   'GLOBAL LOADLIB VTAM VSCS NASEXCAA'
   'LOADCMD VTAM ISTINV00'
        .
        .
        .
```

Restart VTAM

The final step to installation of the Audit SME is to simply restart ACF/VTAM. Naturally, this is an action that should be scheduled within your installation, as appropriate.

When VTAM restarts, the Audit SME will begin to produce messages to the destination(s) you have selected (PUT or WTO). You will receive messages similar to these:

```
NRSFE01 The NRS Audit SME Version 1.0.2, Copyright (c) 1993
NRSFE02   North Ridge Software, Inc.
NRSFE03   1305 11th Street
NRSFE04   Bellingham, Washington 98225
NRSFE05   (360) 676-5999 FAX (360) 733-5970
NRSFE06   IBMMail Exchange US3NN001 IIN NRSI001
NRSFE12 You can obtain a complete SME from NRS called Access, which is a
NRSFE13   portion of The Network Center. Call NRS at (360) 676-5999!
NRSFE14 ISTEXCAA base is 00269008 and SME is at 002CE000
NRSFE10 VM VTAM=VV34 Netid=NRS SSCP=SSCP34 HOSTPU=VTAM34 Address= 34
```

The presence of these messages will indicate that the Audit SME is active. The next output generated will be a function of the customization options selected.

Operation

Operation of the Audit SME is intended to be "exploratory" or temporary in nature. There is certainly nothing to prohibit you from operating it in a production mode, but you should give due consideration to how it will fit into a production environment over a long period (how to process the results, etc.).

Without regard for whether you intend to execute the Audit SME permanently or not, the SME can be configured to produce a variety of output.

Customization

Each option within the Audit SME has a specific "name" that is always referenced in this document in upper case (e.g. PUT indicates the option to send the output to a sysout/printer type file). You will find the individual bit settings in NASOPTS also use these names to indicate how to activate the option.

The Audit SME has the following options set when first unloaded from the tape; **MAXIMUM=10,000, INTVL=3600 (about 1 hour), UNIQUE, INTERVAL, and WTO**. DETAIL, HIERARCHY, PUT, HEXDUMP, and IGNORE are off. QUALIFY is set to monitor every session.

The following options are available in the Audit SME and can be activated as described in each of the following areas:

DETAIL

The **DETAIL** function causes the Audit SME to issue a single message for each session that is presented to the SME for approval.

An example of the message is:

```
NRS0101 Session between NRS SSCP34 T34001 and NRS SSCP32 A32VM
```

This message indicates the SLU's Netid (NRS), SLU's SSCP (SSCP34), SLU (T34001) and the PLU's Netid (NRS), PLU's SSCP (SSCP32) and PLU (A32VM).

You can select the Detail Message for the Secondary Authorization exit point by turning on bit 2 of the DETAIL flag in NASOPTS.

HEXDUMP

The **HEXDUMP** function causes the Audit SME to dump the input parameter list for a specific entry to the Audit SME in a hexadecimal interpreted format.

An example of the output of HEXDUMP for a single entry to the Secondary Authorization exit is:

```
NRS0101 Session between NRS SSCP1 T01006 and NRS SSCP34 A34VM
NRSXX03 01.00 0000 003C0A06 D5D9E240 40404040 0A07E2E2 * ....NRS     ..SSC*
NRSXX03 01.00 0010 C3D7F3F4 40400A08 E5E3C1D4 F3F44040 * CP34  ..VTAM34   *
NRSXX03 01.00 0020 08090000 00220000 0A0AD5D9 E2404040 * ..........NRS    *
NRSXX03 01.00 0030 40400A0B D5D9E240 40404040          *   ..NRS          *
NRSXX03 01.04 0000 01200000                            * ....             *
NRSXX03 01.08 0000 002CE000                            * ..\.             *
NRSXX03 01.12 0000 193D09C0 08E2E2C3 D7F3F440 4008D5D9 * ... .SSCP34  .NRS*
NRSXX03 01.12 0010 E2404040 404008C1 F3F4E5D4 40404008 * S     .A34VM   .N*
NRSXX03 01.12 0020 D5D9E240 40404040 08C1F3F4 E5D44040 * NRS     .A34VM   *
NRSXX03 01.12 0030 401A0800 00002200 0600001A 001A00FF *  ............    *
NRSXX03 01.16 0000 193D0980 08E2E2C3 D7F14040 4008D5D9 * .....SSCP1   .NRS*
NRSXX03 01.16 0010 E2404040 404008E3 F0F1F0F0 F6404008 * S     .T01006  .N*
NRSXX03 01.16 0020 D5D9E240 40404040 08E3F0F1 F0F0F640 * NRS     .T01006  *
NRSXX03 01.16 0030 401A0800 00000100 4F00001A 001A00FF *  .......|........*
NRSXX03 01.20 0000 E9BB3F43 F38869AC D5D9E24B E2E2C3D7 * Z...3h..NRS.SSCP1*
NRSXX03 01.20 0010 F1404040 40404040 40000002          * 1...........     *
NRSXX03 01.36 0000 0908E2E2 C3D7F140 40400000          * ..SSCP1   ..     *
```

This function enables you to cause the Audit SME to dump the precise contents of a VTAM parameter list to the output (WTO or PUT) media. The message is in the form "NRSXX03 ep.pv offset hex *character*" where:

ep is the numeric value internally associated with the Session Management Exit's entry point that is producing the HEXDUMP. This value is equivalent to the function code that has been presented to the Session Management Exit.

pv identifies the decimal offset in the Session Management Exit's parameter list that is being dumped. The Audit SME will print all arguments within the parameter list that are defined for the entry point that has been called.

offset contains the hexadecimal offset in storage from the beginning point of a particular address pointer.

hex the actual hexadecimal information stored at the designated location.

character the hexadecimal information converted to common EBCDIC values (the text may or may not be meaningful).

Note: This option will produce **large volumes of output** for most VTAM systems and should **not be used unless you are specifically testing a particular situation**.

HIERARCHY

The **HIERARCHY** function requests that the Audit SME interpret each LU entering a session and displays the definition hierarchy associated with the LU.[4] HIERARCHY will produce output only if DETAIL is also activated.

The HIERARCHY output will always follow NRS0101 and will appear similar to:

```
NRS0102   SLU hierarchy T32001 LU
NRS0102   SLU hierarchy T32L Local non-SNA major node
NRS0102   PLU hierarchy A32VM APPL
NRS0102   PLU hierarchy T32NRS APPL major node
```

These messages produce an excellent audit trail of precisely the sequence of definitions used to identify the LU. However, this can produce a large volume of output for a VTAM that is active and should be used cautiously.

This function defaults to off and is activated by turning on bit 8 of FLAG1 (the HIERARCHY bit).

IGNORE

The **IGNORE** option instructs the Audit SME to issue a message when the QUALIFY fields have caused a session to be ignored within the Audit SME.[5]

An example of the output is:

```
NRS0111 Ignoring Netid=NRS Sscp=SSCP34 Lu=T34001
```

The Audit SME will "ignore" the fact that the session occurred whether the IGNORE option is on or off. IGNORE simply causes a message to be produced when a session is ignored.

This option is normally off and can be activated by turning on bit 3 of FLAG1 (the IGNORE bit).

---

[4] This function utilizes control blocks that may not be available on some releases of VTAM (i.e. prior to VTAM 3.4).

[5] The Audit SME always sends the proper return code back to VTAM to allow the session to continue. "Ignore" means only that the Audit SME will not count the session in its computations.

INTERVAL

The **INTERVAL** function causes the Audit SME to issue a message for each unique Netid and Subarea it has encountered on a timed basis (the period of time is defined by the INTVL option).

An example of these messages are:

```
NRS0108 Total sessions since 92.140 at 15:51:23= 2,321, 92.140 18:33:21= 345
NRS0110   NRS SSCP32= 1,923 Plu= 823 Slu= 1,100 Interval 301
NRS0110   NRS SSCP34= 398 Plu= 324 Slu= 74 Interval 344
```

These messages are issued by the Audit SME when the number of timer units specified in INTVL has elapsed (1 timer unit approximates 1 elapsed second) since the last time the Audit SME issued these messages. The Audit SME will issue the messages when it is entered to approve a session. Therefore, if the Audit SME is not entered (VTAM is basically inactive with sessions) then the messages may have an interval longer than INTVL.

Note: The NRS0110 message is repeated once for each unique SSCP and network that the Audit SME has encountered. The NRS0108 session counts are the number of times the Audit SME has received control in the Session Authorization exit. The NRS0110 counts are "half session" counts that show how many times the particular domain has been involved in a session as a SLU and/or PLU. If the local domain has both the SLU and the PLU domain, then the NRS0110 count will be 2.

Activate the interval recording by turning on bit 6 of the FLAG1 byte (the INTERVAL option).

INTVL

The **INTVL** binary fullword contains the quantity of processor "timer units" that will elapse between summary messages indicating the volumes of activities that have occurred. This value is approximately equal to the number of seconds desired between output messages (it is the "interval" between the INTERVAL messages).

INTVL is a binary fullword that defaults to X'E10' or approximately 3,600 seconds (1 hour). Do **not** set a very small INTVL or you will generate a large volume of output messages.[6]

MAXIMUM

The **MAXIMUM** fullword contains the number of output messages that the Audit SME will produce before it terminates the output of additional messages. This is intended to be a "governor" to prohibit the output lines from exceeding a limit that you set.

The default is 10,000 output lines, but you should set MAXIMUM to a value that is acceptable to your installation for its purposes.

---

[6] Remember the INTERVAL logic is intended to give you an overview of your system's volumes.

OPTIONS

The **OPTIONS** bits allow you to specify which specific Session Management Exit exit points that the NRS Audit SME will receive control for. The OPTIONS bit string is the bytes that will be used by the Audit SME to set the BEGIN function response.

As shipped, the NRS Audit SME has activated the Session Authorization exit point, which should satisfy most purposes for using the Audit SME.

PUT

The **PUT** option instructs the Audit SME to OPEN the NASLOG DCB and place the output messages into the DD or FILEDEF. This can be used to send the output messages to a standard SYSOUT/PRINTER file or into a disk data set/file.

Note: The PUT option uses QSAM to output the messages and has no error recovery associated will filling up a disk dataset or CMS mini-disk. If this occurs, the Audit SME will suffer an operating system interrupt and may be disabled by ACF/VTAM (ACF/VTAM itself will continue to operate normally).

The Audit SME has been built to generally accept and operate properly in 31 bit addressing mode. However, the sequential access routines used to output to the NASLOG DD statement do **not properly operate** in 31 bit addressing mode (processing associated with a conventional DCB). Therefore, you should link the Audit SME in 24 bit AMODE if you intend to activate the PUT option.

QUALIFY

You can select or **QUALIFY** which items in your network that you would like the Audit SME to count, display, etc. by setting one or more of the QUALIFY selection fields. You can set the value of:

Field	*Contents*
PLU	the Primary Logical Unit name (typically, the subsystem)
PLU-SSCPNAME	the origin SSCP for the PLU
PLU-NETID	the origin Network for the PLU
SLU	the Secondary Logical Unit name (the terminal device)
SLU-SSCPNAME	the origin SSCP for the SLU
SLU-NETID	the origin Network for the SLU

Figure 6. QUALIFY Values

The QUALIFY values are all 8 character fields that can be "pattern matched" with the following characters:

***** all characters match without regard for the number of characters

% any single character matches

The string "T01*" indicates any item that starts with the letters "T01" will match. "T01%" indicates that any item whose name is exactly four characters long and starting with "T01" will match. "T*4" will match any item that starts with a "T" and ends with a "4".

The QUALIFY fields must all allow a specific session to be counted in order for the session to be reported (i.e. the select fields are logically ANDed together). Setting PLU-NETID to "NRS" and SLU-SSCPNAME to "ADMIN*" will cause the Audit SME to report only on sessions where the device (SLU) is a SSCP that starts with ADMIN and the subsystem (PLU) is in the Network named NRS.

The default values for all the QUALIFY fields is a a single asterisk ("*") so that everything will match.

UNIQUE

The **UNIQUE** function causes the Audit SME to issue a message for each unique Netid and Subarea it encounters. Only one message for each unique subarea/netid combination is issued. An example of the message is:

```
NRS0106 New node recognized, Network=NRS Sscp=SSCP1 Subarea= 1
```

This option is useful to identify the nodes that your VTAM domain either initiates contact with or is contacted by. It is an excellent way to summarize the network activities your VTAM is involved with.

Activate the Unique Combination by turning on bit 7 of the FLAG1 byte (the UNIQUE option).

WTO

The **WTO** option instructs the Audit SME to output each message to the main console for information (the VTAM virtual machine's console for VM systems). This option defaults to on and can be disabled by turning off bit 5 of FLAG1 (the WTO bit).

If you leave WTO enabled, exercise care about activating any option that will generate a large number of messages. This combination can cause the operator's console to be "flooded" with messages if your VTAM system is very active!

Messages

The Audit SME's message identifiers are in the general form **NRSxxnn**, where:

NRS	a constant identifying the message as originating from the Audit SME
xx	is a hexadecimal representation of the Session Management Exit function code that received control (FE is the Begin function code, FF is the End function code, 00 is the Initial Authorization function, etc.)
nn	a numeric value that uniquely identifies the message within the Audit SME's functional code processing a specific function code

Figure 7. Message Number Format

The message text will have variable information filled in by the Audit SME during execution. This "variable information" is represented by a brief descriptor enclosed in special symbols such as <sample>.

NRSFE01 The NRS Audit SME Version <version>, Copyright (c) 1993

NRSFE02 North Ridge Software, Inc.

NRSFE03 1305 11th Street

NRSFE04 Bellingham, Washington 98225

NRSFE05 (360) 676-5999 FAX (360) 733-5970

NRSFE06 IBMMail Exchange US3NN001 IIN NRSI001

NRSFE10 <system> VTAM=<vtam version> Netid=<netid> SSCP=<sscpname> HOSTPU=<hostpu>

NRSFE12 You can obtain a complete SME from NRS called Access, a

NRSFE13 portion of The Network Center. Call NRS at (360) 676-5999

NRSFE14 ISTEXCAA based is <address> and SME is at <address>

NRSFF01 Terminate is complete, Contact NRS for additional information about SMEs!

NRSXX01 Output message maximum encountered, output terminated

NRSXX02 Invalid RIC length

NRSXX03 <exit>.<argument> <offset> <hexadecimal value of argument>

NRS0001 Initial Authorization Exit invoked

NRS0101 Session between <netid> <sscp> <slu> and <netid> <sscp> <plu>

NRS0102 SLU hierarchy <resource> <resource description>

NRS0103 PLU hierarchy <resource> <resource description>

NRS0104 ILU is <netid> <applname>

NRS0105 ILU hierarchy <resource> <resource description>

NRS0106 New node recognized, Network=<netid> Sscp=<sscp> Subarea=<subarea>

NRS0107 Internal accumulation area overflow, accumulation terminated

NRS0108 Total sessions since <date> at <time>= <number>, <date> <time>= <number>

NRS0110 <netid> <subarea>= <number> Plu=<number> Slu=<number> Interval=<number>

NRS0111 Ignoring Netid=<netid> Lu=<luname>

NRS0112 Unidentified parameter list

NRS0201 Initial Accounting Exit invoked

NRS0301 Final Accounting Exit invoked

NRS0401 Gateway Path Selection Exit invoked

NRS0501 XRF Session Switch Exit invoked

NRS0601 Adjacent SSCP Selection Exit invoked

NRS0701 Alias Selection Exit invoked

NRS0801 Adjacent Link Station Selection exit invoked

NRS0901 Exit replacement exit invoked

NRS0A01 Exit replaced exit invoked

NRS0B01 Virtual Route Selection exit invoked

Appendix A. Sample Output

The following listing of the Audit SME was collected by extracting only the Audit SME's messages from a spooled virtual console in VM operating a copy of VTAM 3.4. The DETAIL, HIERARCHY, UNIQUE, INTERVAL, WTO, and PUT options were on. The QUALIFY values were set to include any SLU that ended with a 6 (SLU=*6).

```
NRSFE01 The NRS Audit SME Version 1.0.2, Copyright (c) 1993
NRSFE02   North Ridge Software, Inc.
NRSFE03   1305 11th Street
NRSFE04   Bellingham, Washington 98225
NRSFE05   (360 676-5999 FAX (360) 733-5970
NRSFE06   IBMMail Exchange US3NN001 IIN NRSI001
NRSFE12 You can obtain a complete SME from NRS called Access, which is a
NRSFE13   portion of The Network Center. Call NRS at (360) 676-5999!
NRSFE14 ISTEXCAA base is 00269008 and SME is at 002CE000
NRSFE10 VM VTAM=VV34 Netid=NRS SSCP=SSCP34 HOSTPU=VTAM34 Address= 34
NRS0106 New node recognized, Network=NRS Sscp=SSCP1 Subarea= 1
NRS0106 New node recognized, Network=NRS Sscp=SSCP34 Subarea= 34
NRS0101 Session between NRS SSCP1 T01006 and NRS SSCP34 A34VM
NRS0102   SLU hierarchy T01006 CDRSC
NRS0102   SLU hierarchy ISTCDRDY CDRSC major node
NRS0103   PLU hierarchy A34VM APPL
NRS0103   PLU hierarchy A34NRS APPL major node
NRS0101 Session between NRS SSCP1 T01006 and NRS SSCP34 A34VM
NRS0102   SLU hierarchy T01006 CDRSC
NRS0102   SLU hierarchy ISTCDRDY CDRSC major node
NRS0103   PLU hierarchy A34VM APPL
NRS0103   PLU hierarchy A34NRS APPL major node
NRS0111 Ignoring Netid=NRS Sscp=SSCP34 Lu=T34001
NRS0101 Session between NRS SSCP34 T34006 and NRS SSCP34 A34VM
NRS0102   SLU hierarchy T34006 LU
NRS0102   SLU hierarchy T34L Local non-SNA major node
NRS0103   PLU hierarchy A34VM APPL
NRS0103   PLU hierarchy A34NRS APPL major node
NRS0108 Total sessions since 92.227 at 7:32:16= 4, 92.227 at 7:32:16= 4
NRS0110   NRS SSCP1 = 2 Plu= 0 Slu= 2 Interval= 2
NRS0110   NRS SSCP34 = 4 Plu= 3 Slu= 1 Interval= 4
NRS0111 Ignoring Netid=NRS Sscp=SSCP1 Lu=T01008
NRSFF01 Termination is complete, Contact NRS for information about SMEs!
```

Appendix B. NRS Audit SME Options Member/File

The following sample NASOPTS is present on the distribution tape and can be used as input to the SuperZap service aid to set the Audit SME options.

```
* ------------------------------------------------------------------ *
*                                                                    *
*  NRS Audit SME - Execution options                                 *
*                                                                    *
*  You may use some or all of these options, as you deem appropriate. *
*  Reference the documentation (NAS0023) for details.                *
*                                                                    *
*  An asterisk in column one makes the entire line a comment!        *
*                                                                    *
* ------------------------------------------------------------------ *
NAME ISTEXCAA ISTEXCAA
VER 001D F14B,F04B,F290                      *** VERSION 102  ***
*REP 00C6 4000       B'0100000000000000'     *** OPTIONS      ***
*REP 00C8 0000       B'0000000000000000'     *** DETAIL       ***
*REP 00CA 0000       B'0000000000000000'     *** HEXDUMP      ***
REP 00CC 0000,2710   F'10000'                *** MAXIMUM      ***
REP 00D0 0000,0E10   F'3600' <-ABOUT 60 MINS *** INTVL        ***
*
*                        Ignore              *** IGNORE       ***
*                        |Put                *** PUT          ***
*                        ||Wto               *** WTO          ***
*                        |||Interval         *** INTERVAL     ***
*                        ||||Unique          *** UNIQUE       ***
*                        |||||Hierarchy      *** HIERARCHY    ***
*                        ||||||
REP 00D4 0E          B'00001110'             *** FLAG1        ***
*
*                                            *** QUALIFY      ***
REP 00D5 5C40,4040,4040,4040                 *** SLU          ***
REP 00DD 5C40,4040,4040,4040                 *** SLU-SSCPNAME ***
REP 00E5 5C40,4040,4040,4040                 *** SLU-NETID    ***
REP 00ED 5C40,4040,4040,4040                 *** PLU          ***
REP 00F5 5C40,4040,4040,4040                 *** PLU-SSCPNAME ***
REP 00FD 5C40,4040,4040,4040                 *** PLU-NETID    ***
```

Appendix C. Bibliography

The following IBM publications are useful in conjunction with ACF/VTAM. The applicable *Customization* guide contains the majority of the documentation about the Session Management Exit.

Publication Title

GA27-3136 SNA Reference Summary

SC23-0111 Installation and Resource Definition

SC23-0115 VTAM Programming

LY43-0081 Network Product Formats

GG24-3544 Network Security Using the VTAM Session Management Exit

VTAM 3.1.1

The following publications are specific to ACF/VTAM version 3.1.1:

Publication Title

SC23-0116 VTAM Diagnosis Guide

LY30-5582 VTAM Diagnosis Reference

LY30-5583 VTAM Data Areas for VM

LY30-5584 VTAM Data Areas for MVS

SC23-0135 VTAM Reference Summary

SC23-0112 Customization

VTAM 3.2

The following publications are specific to ACF/VTAM version 3.2:

Publication	*Title*
LY30-5601	VTAM Diagnosis
LY30-5593	VTAM Data Areas for VM
LY30-5594	VTAM Data Areas for MVS
LY30-5600	VTAM Reference Summary
LD35-0270	VTAM V3R2 Enhancements
LY30-5614	Customization

VTAM 3.3

The following publications are specific to ACF/VTAM version 3.3:

Publication	*Title*
LY43-0042	VTAM Diagnosis
LY43-0045	VTAM Data Areas for VM
LY43-0043	VTAM Data Areas for MVS
LY43-0047	VTAM Reference Summary

VTAM 3.4

The following publications are specific to ACF/VTAM version 3.4:

Publication	*Title*
LY43-0059	VTAM Diagnosis
LY43-0058	VTAM Data Areas for VM
LY43-0057	VTAM Data Areas for MVS
LY43-0060	VTAM Reference Summary
LY43-0046	Customization

Appendix D. Summary of Changes

The NRS Audit SME is a "work in progress" that will continue to evolve based upon feedback received from those using it to answer their own questions. The following information identifies the evolution of the routine:

Version ***Contents***

1.0.0 Original availability in May 1992

1.0.1 General availability in August 1992

- Replaced use of Subarea with SSCP name in most key areas (including DETAIL and INTERVAL messages)
- Implemented HEXDUMP options for parameter lists
- Ignored session setup failures (accumulation statistics are improperly impacted with failed sessions)
- Automatically hex dumps invalid parameter lists or control vectors

1.0.2 General availability in May 1993.

- Created diskette based distribution
- Corrected NASOPTS offset specifications
- Added OPTIONS bit settings

Glossary

ACF/VTAM: a software offering from IBM that operates on a host mainframe and implements SNA concepts for the teleprocessing equipment

ALIAS: a name used in a host to represent a logical unit, etc. in another network to guarantee a unique value amongst network nodes.

CPU: an acronym for Central Processing Unit, identifies the physical hardware executing instructions

cross domain: describes an action or activity that occurs between two or more domains (E.G. a "cross domain" session is a session where the PLU and SLU are owned by different ACF/VTAM domains).

cross network: describes an action or activity that occurs between two or more SNA networks (E.G. a "cross network" session is a session where the PLU and SLU are owned by different SNA networks).

CSECT: an acronym for Code SECTion, identifies a sequence of 370 assembler instructions that make up a software program

domain: the hardware and software components that make up a single VTAM's authority area within the network

gateway: the combination of machines and programs that provide address translation, name translation, and SSCP rerouting between independent SNA networks

GCS: Group Control System, an acronym for a component of VM/SP that provides for a multi-tasking environment for the execution of ACF/VTAM

LU: Logical Unit, an acronym that identifies a end point in a SNA session (usually a terminal device, but can also identify a program)

MVS: Multiple Virtual Storages, an acronym for the most recent variation of IBM's OS operating system

NETID: The Network Id is a 1 to 8 character string that identifies one or more domains that are operating as a single SNA network

Netview: IBM's VTAM based network management software offering

network: the combination of hardware, software, and interconnection techniques that allow individuals access to information stored on one or more CPUs

operating system: the software offering that manages the physical resources of the host computer (MVS, VM, and DOS are the prevalent IBM offerings).

PLU: Primary Logical Unit, is a SNA term used to identify one "side" of a session (typically, a processing subsystem). Can also be referenced as the Destination Logical Unit or DLU.

PU: Physical Unit, an acronym for one of three types of network addressable unit (NAU). A logical unit, physical unit, or a system services control point

RIC: Resource Identifier Control vector, contains key information about a logical unit

SDLC: Synchronous Data Link Control, an acronym for a definition of the communications procedures between two teleprocessing end points

Session management exit: a provided exit point within ACF/VTAM that allows local installation control over the actions of ACF/VTAM. The routine is also known as ISTEXCAA. (E.G. a "cross network" session is a session where the PLU and SLU are owned by different SNA networks).

SLU: Secondary Logical Unit, is a SNA term used to identify one "side" of a session (typically, the terminal device end of the session). Can also be referenced as the Origin Logical Unit or OLU.

SNA: System Network Architecture, an acronym for the definition of work flow and corresponding units of work between two end points in a teleprocessing connection

SNI: SNA Network Interconnect, an acronym for the connection, by gateways, of two or more independent SNA networks

Subarea: The numeric value that represents a unique processing location (host or front end processor) within the SNA network

subsystem: identifies a ACF/VTAM processing APPLICATION (CICS, TSO, CMS, IDMS, MODEL204, ROSCOE, Netview, etc. are subsystems)

SSCP: System Services Control Point, the key processing point within a ACF/VTAM domain that manages session initiation and termination

terminal: an end user's device for accessing the network and processing information

VM: Virtual Machine, an acronym for an IBM operating system oriented primarily to providing time sharing type services

VTAM: Virtual Telecommunications Access Method, an acronym for an IBM program product that provides network support services to the operating system.

Index

I

L

M

N

O

P

Q

R

S

T

U

V

W