Novell®

Workgroup Partner Engineering Services

Linux OES2
NSS Auditing (“vigil”)

Adam Jerome
Sr. Software Engineer
abj@novell.com

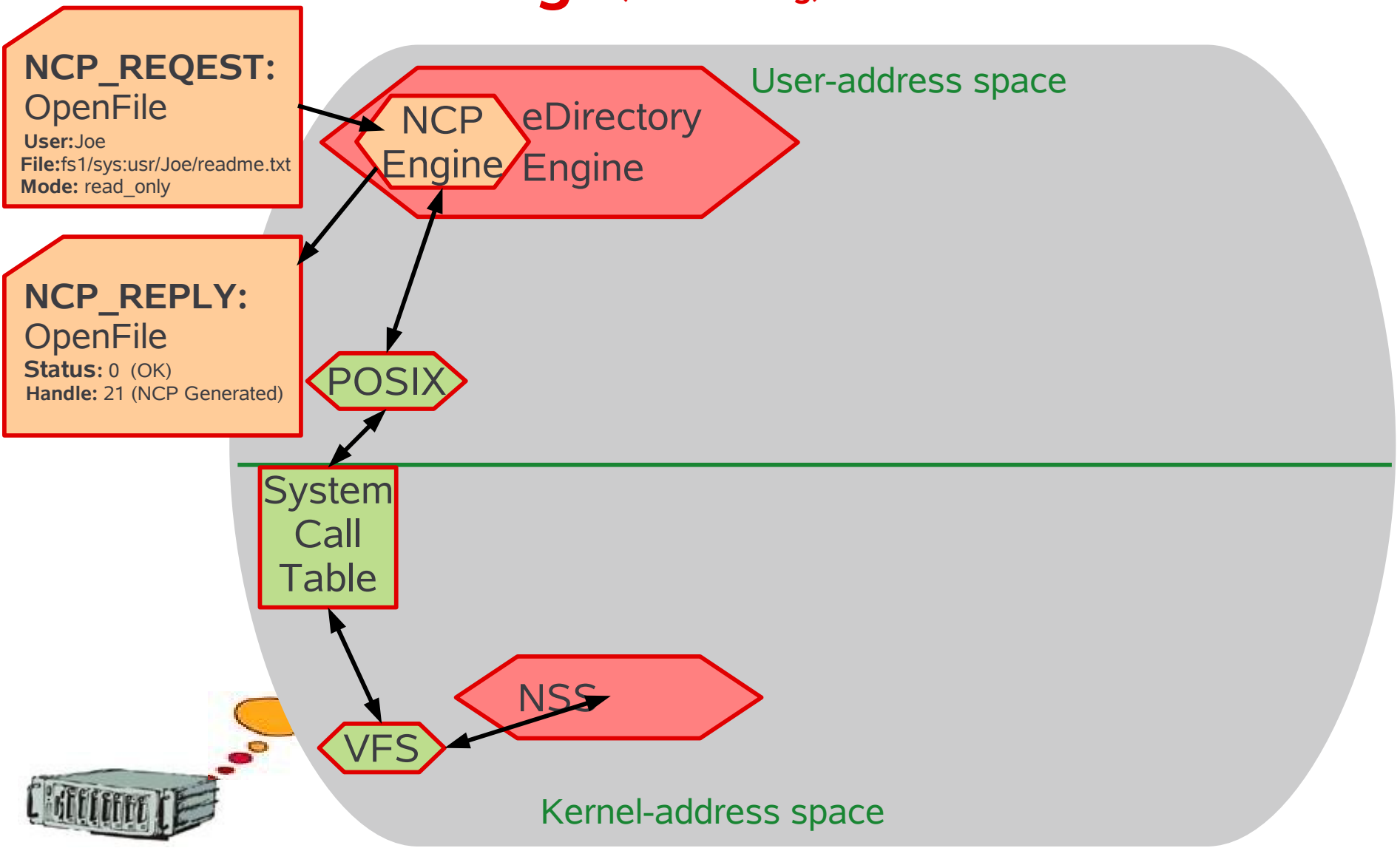
Rev. 2009.08.31

Novell®

UNIT ONE

Linux OES2 Auditing Engine Overview

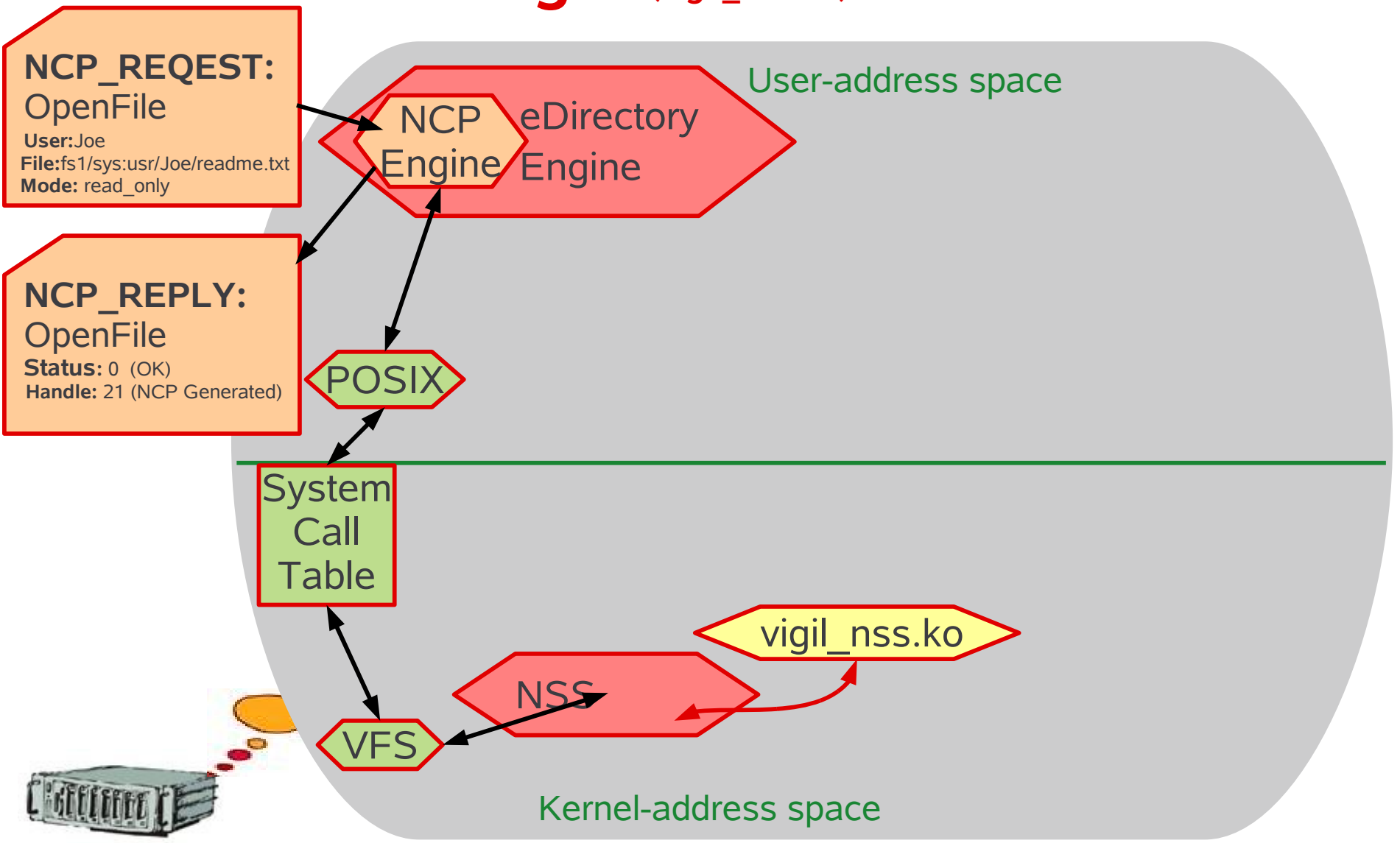
NCP Handling ...(w/o auditing)



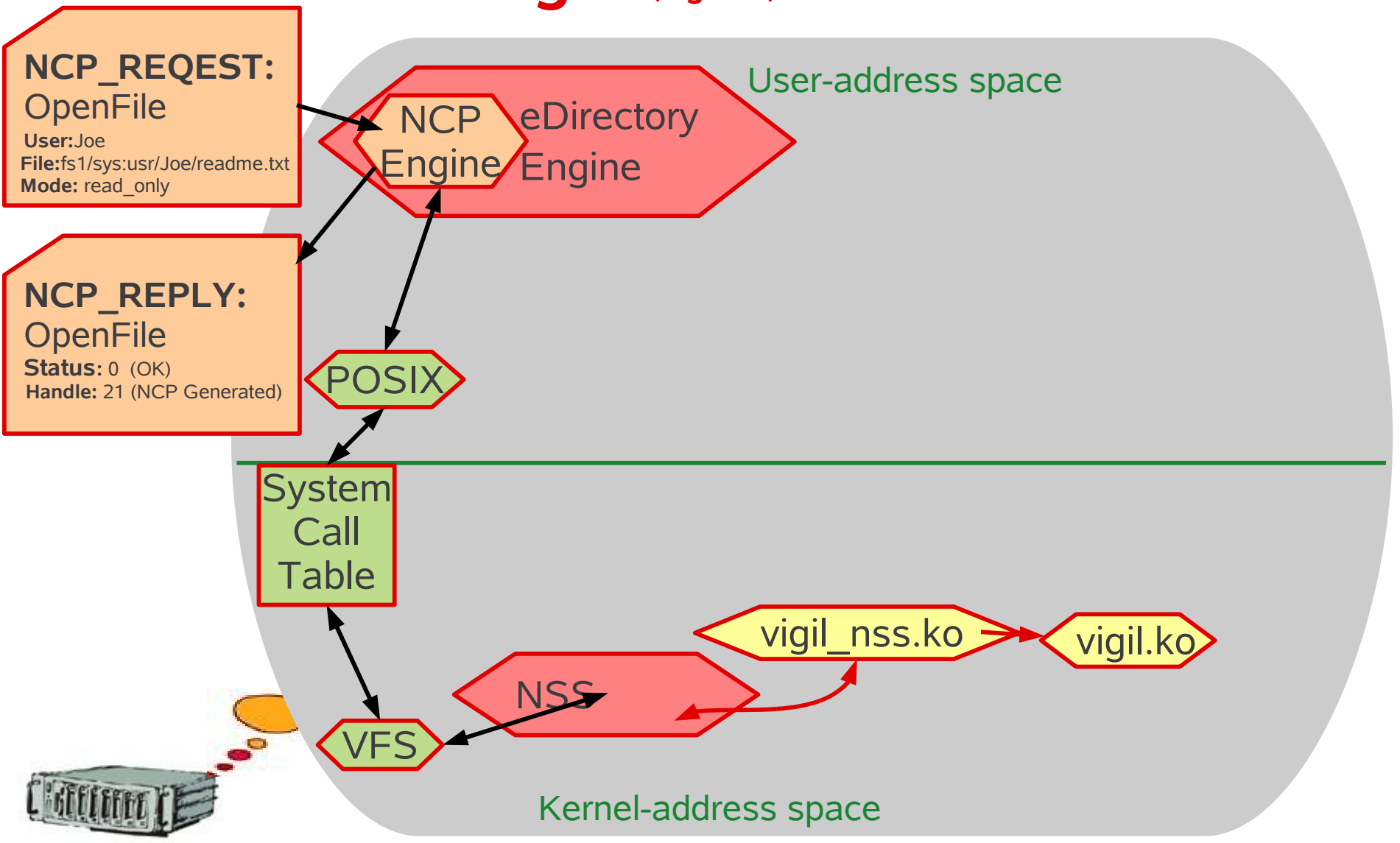
NCP Handling

ADD AUDITING....

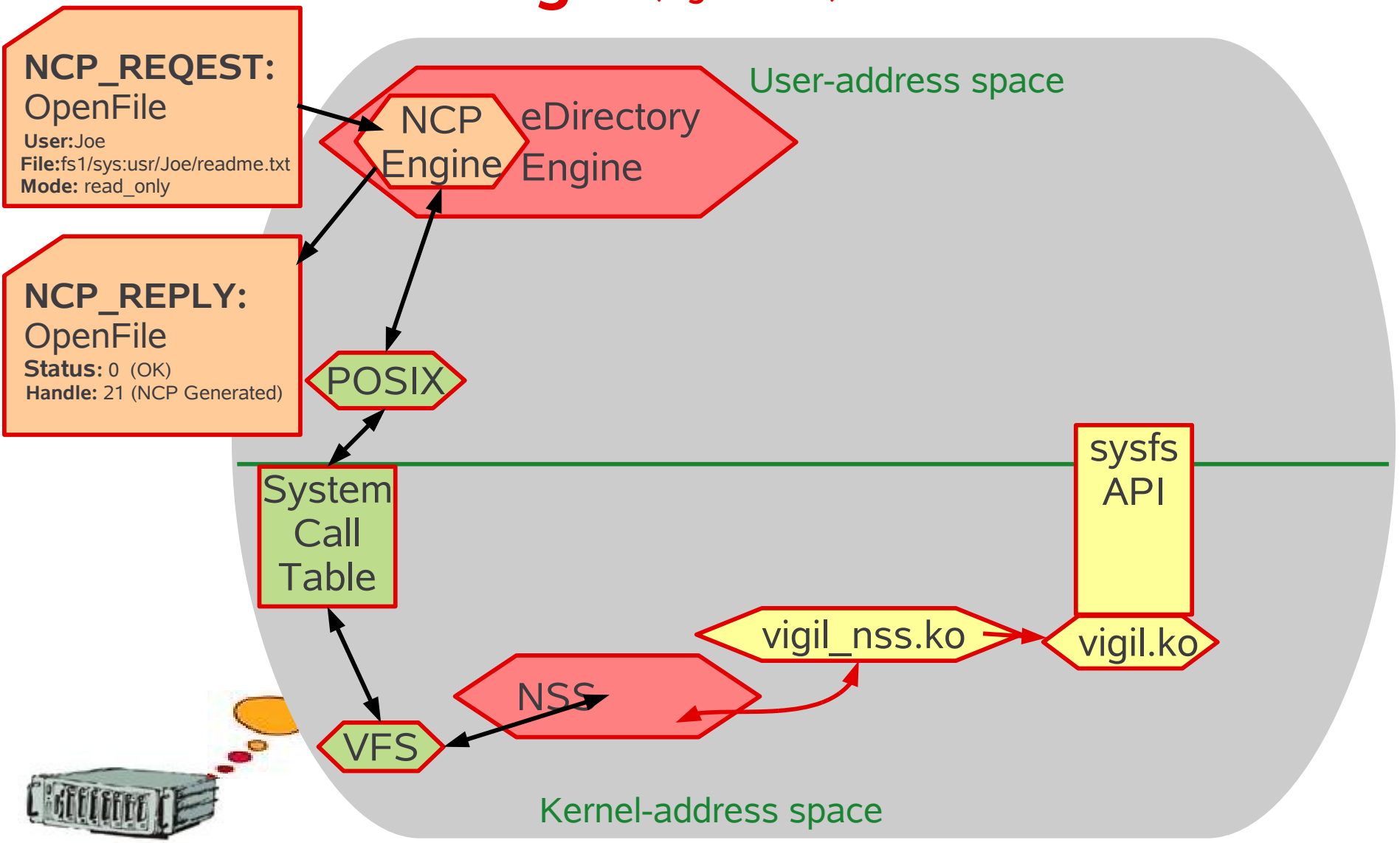
NCP Handling ...(vigil_nss.ko)



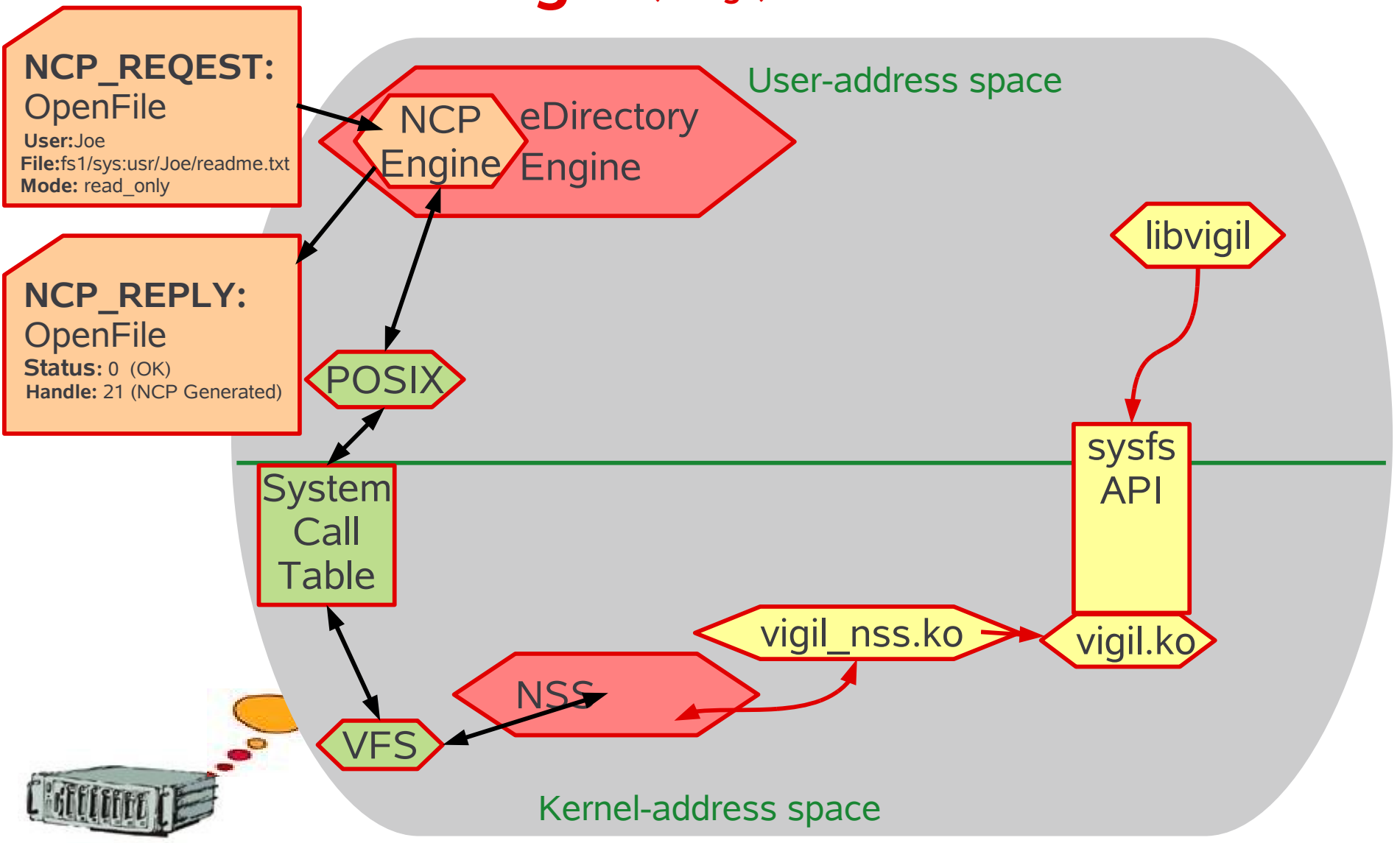
NCP Handling ...(vigil.ko)



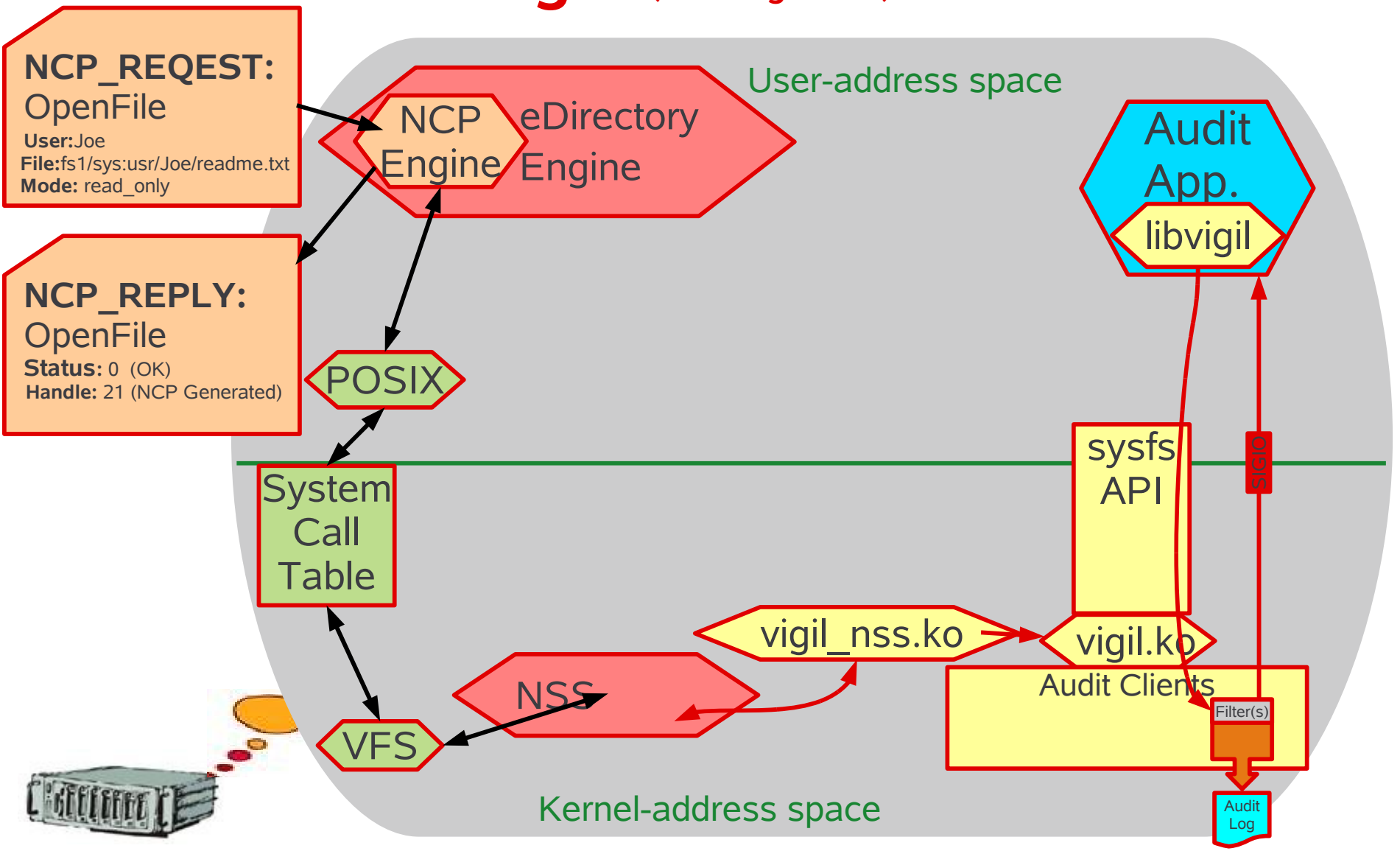
NCP Handling ...(vigil.ko API)



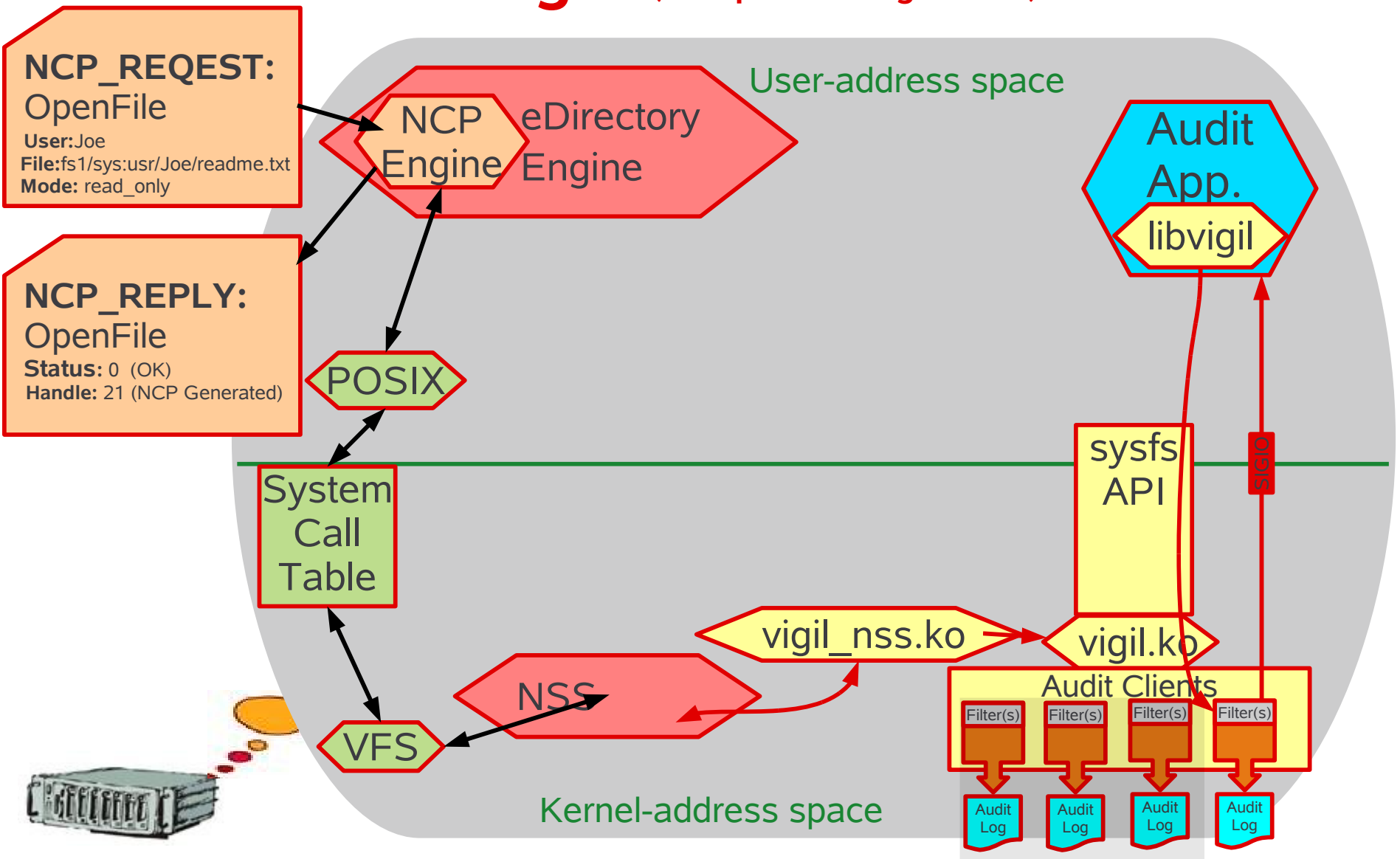
NCP Handling ...(libvigil)



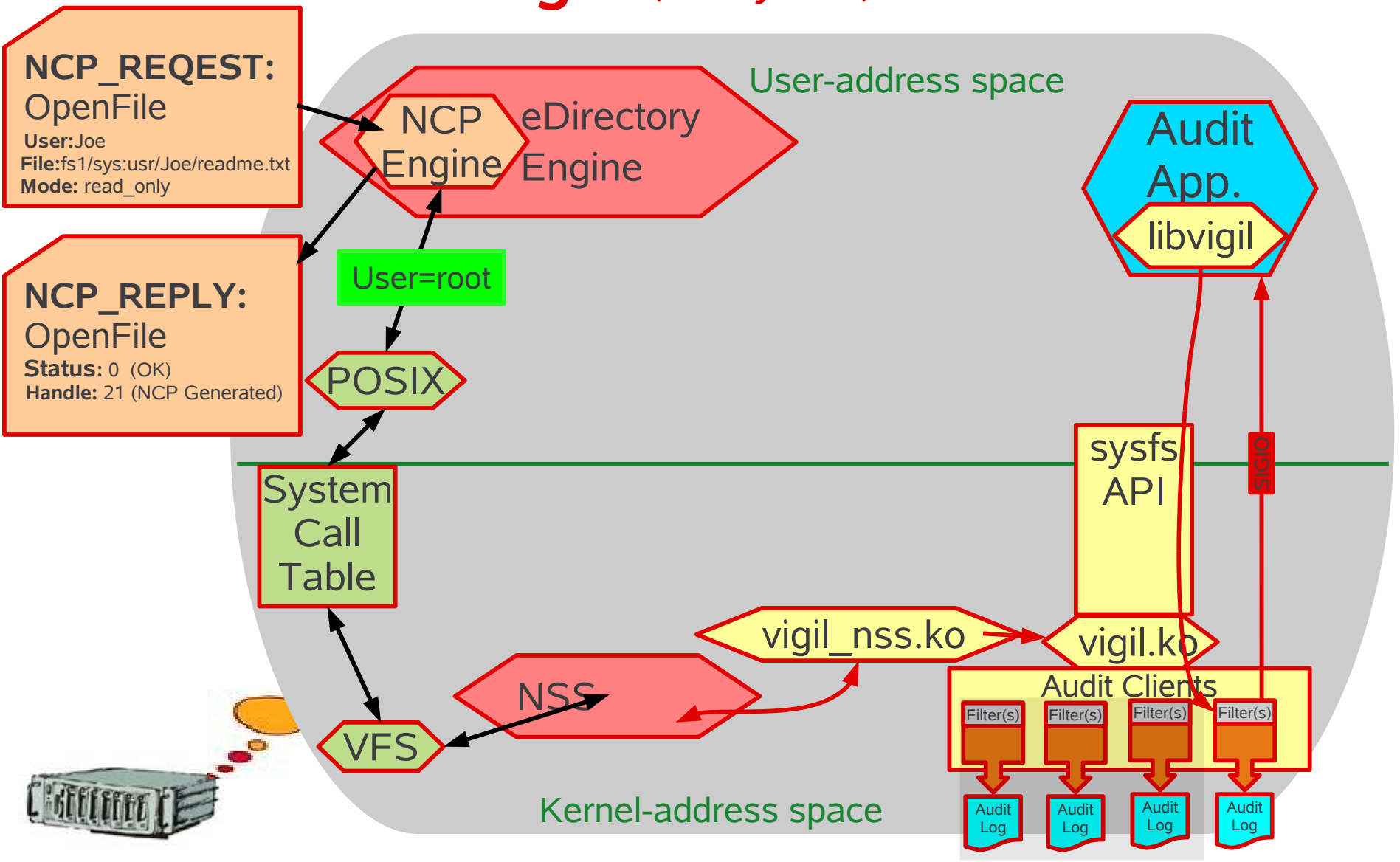
NCP Handling ...(Auditing Client)



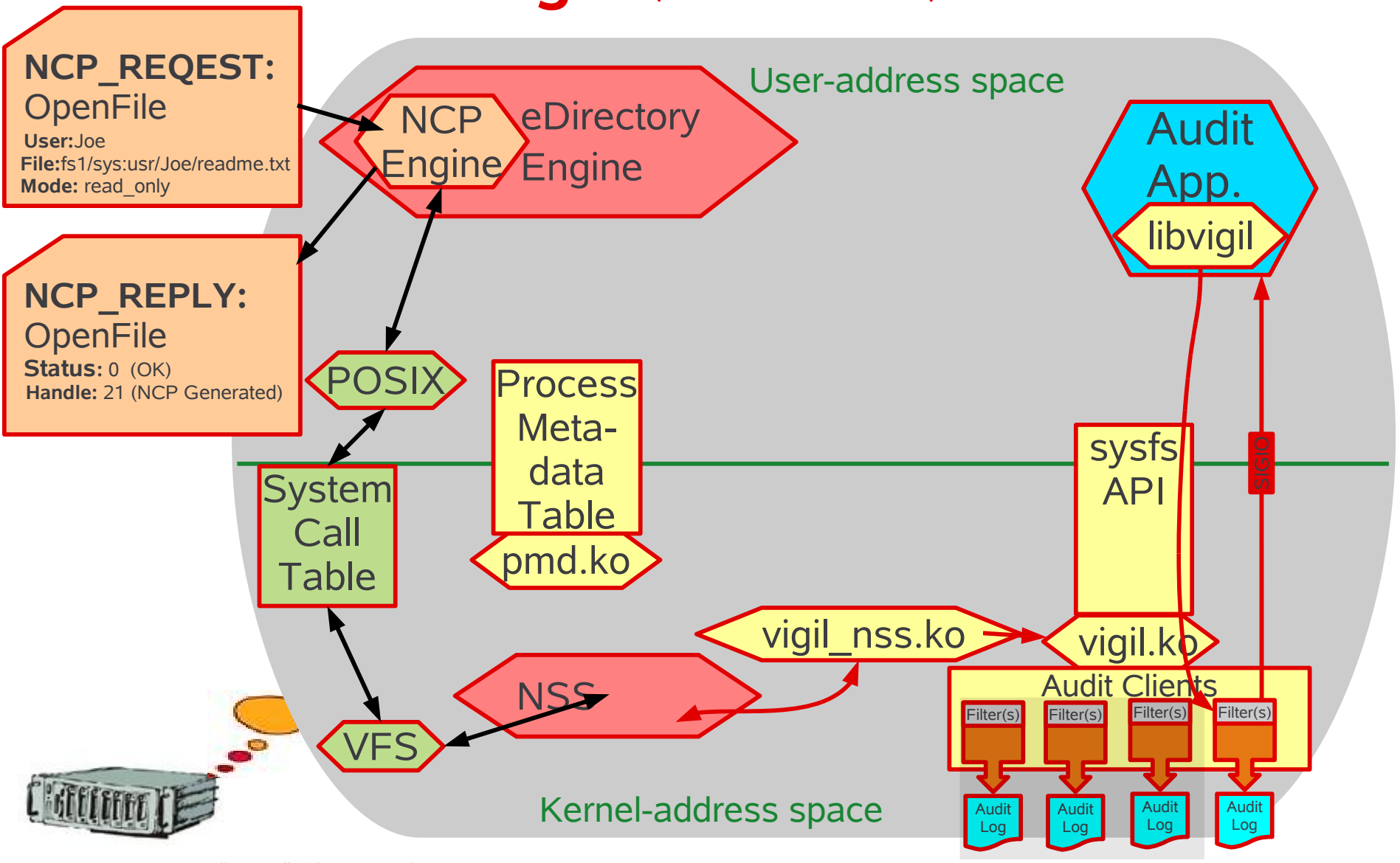
NCP Handling ...(Multiple Auditing Clients)



NCP Handling ...(Identity Issue)



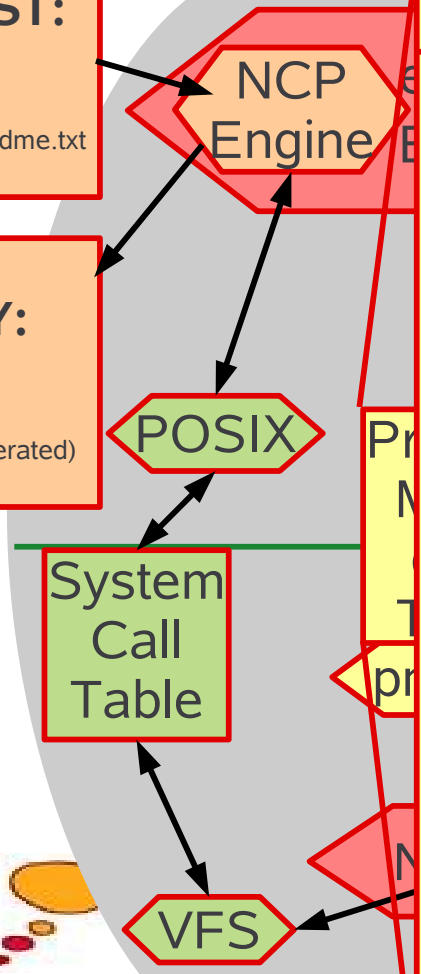
NCP Handling ...(Process Metadata)



NCP Handling ...(Process Metadata Table)

NCP_REQEST:
OpenFile
User: Joe
File:fs1/sys:usr/Joe/readme.txt
Mode: read_only

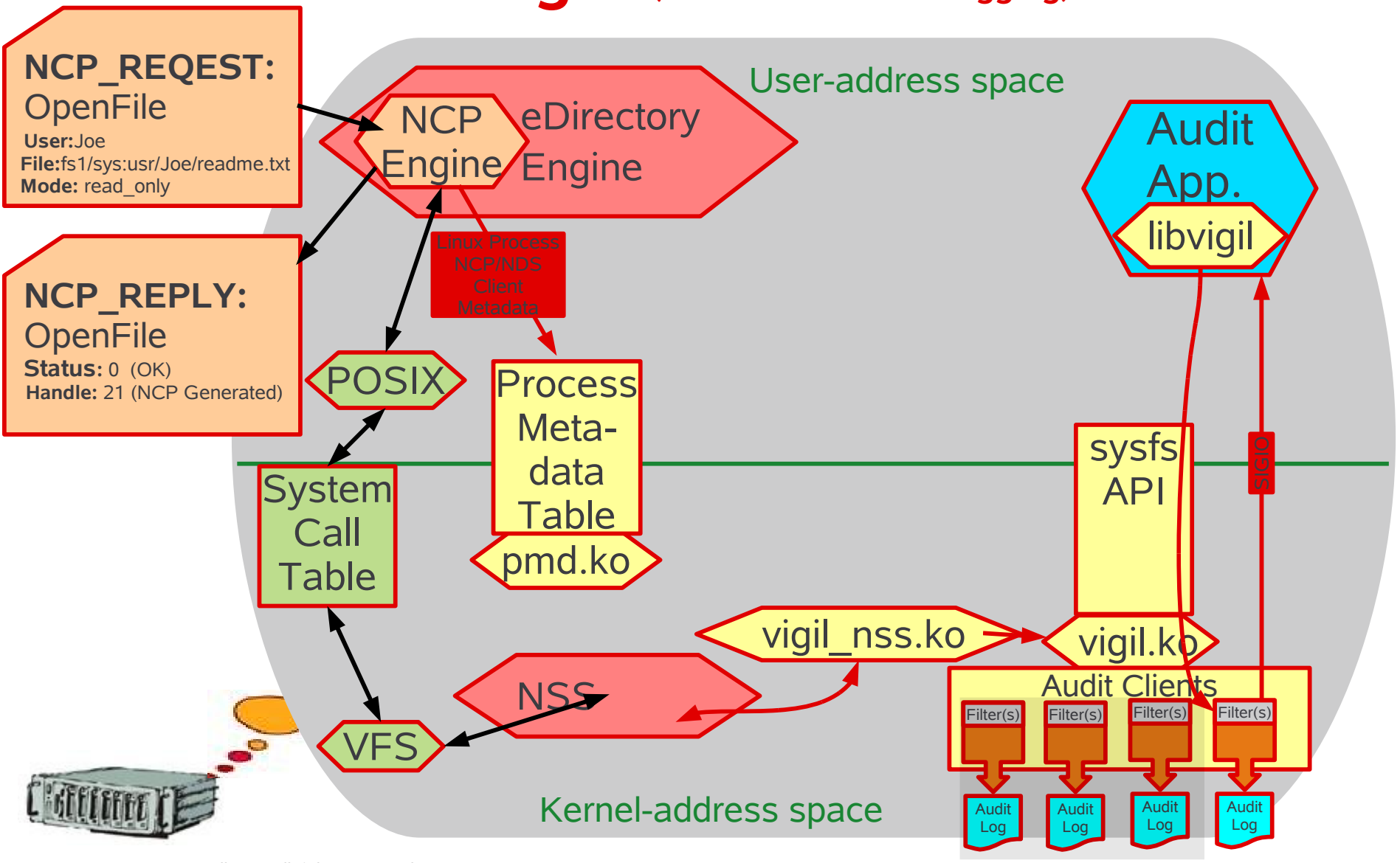
NCP_REPLY:
OpenFile
Status: 0 (OK)
Handle: 21 (NCP Generated)



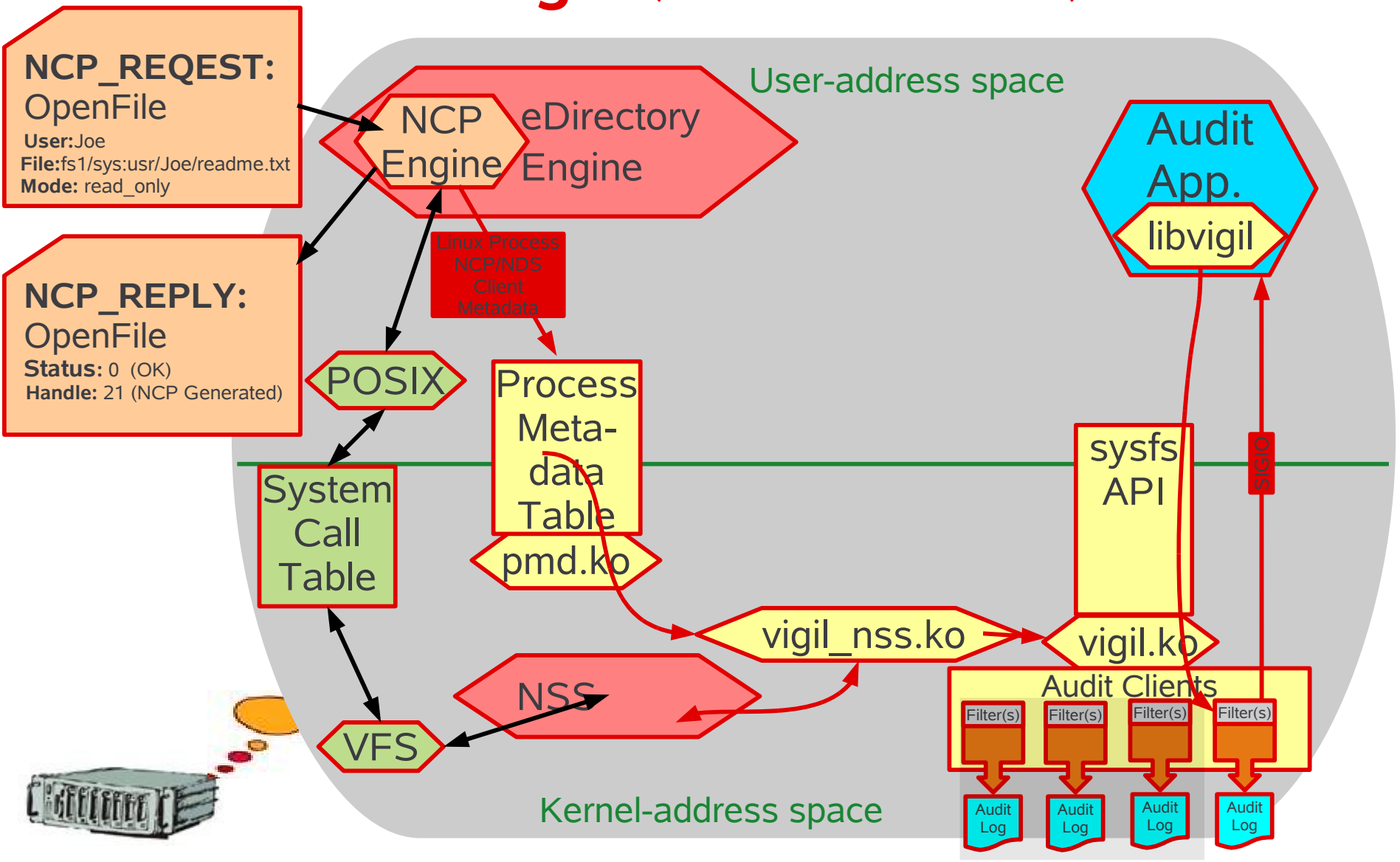
Process Metadata Table

PID	NCP Conn#	NCP Task#	NDS GUID
10532	12	3	FE46A399BD8C
12099	252	24	9CAD53B412EE
2533	85	1	502DFE7A3C10
11300	4	3	DEADBEEF111

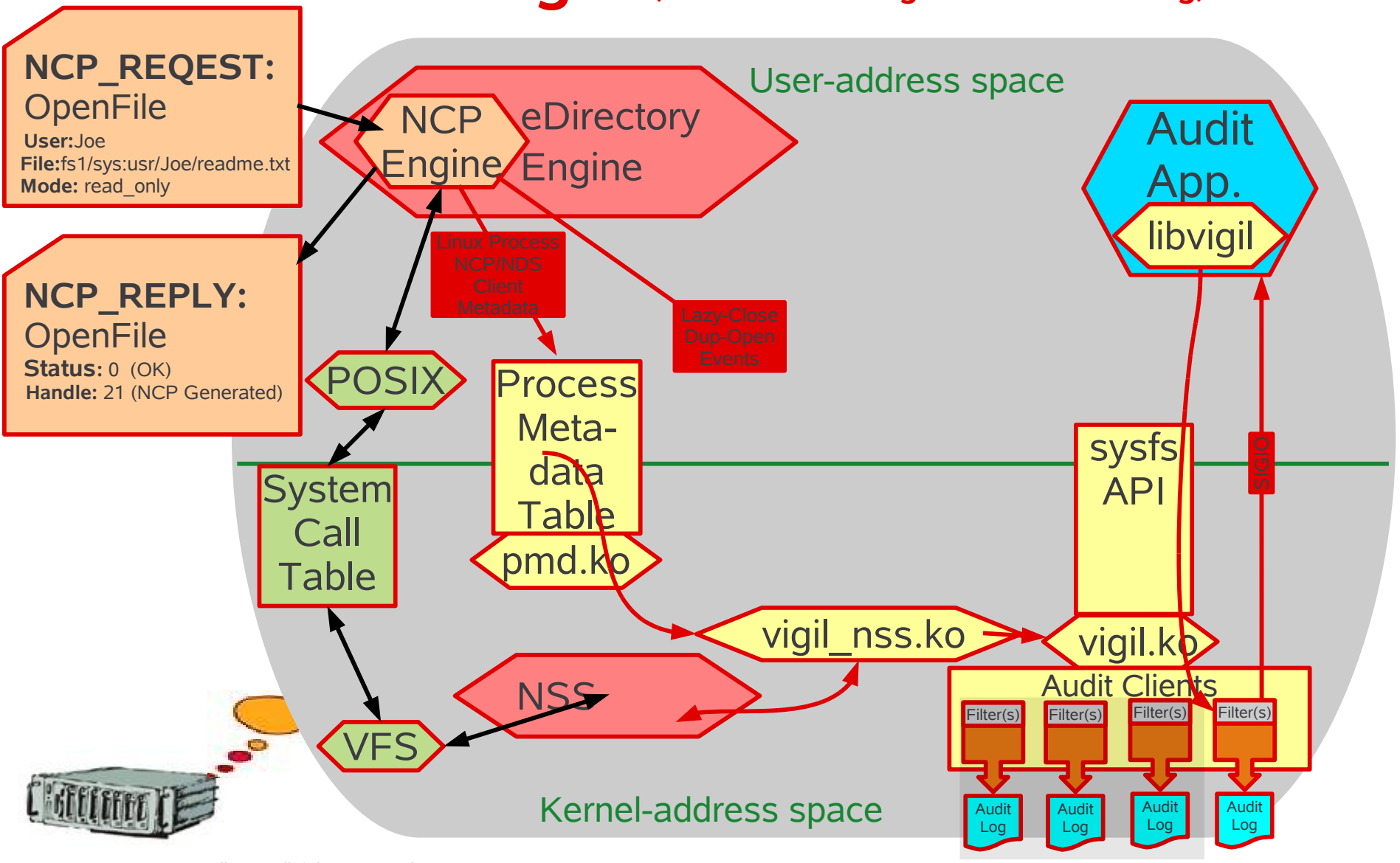
NCP Handling ...(Process Metadata Logging)



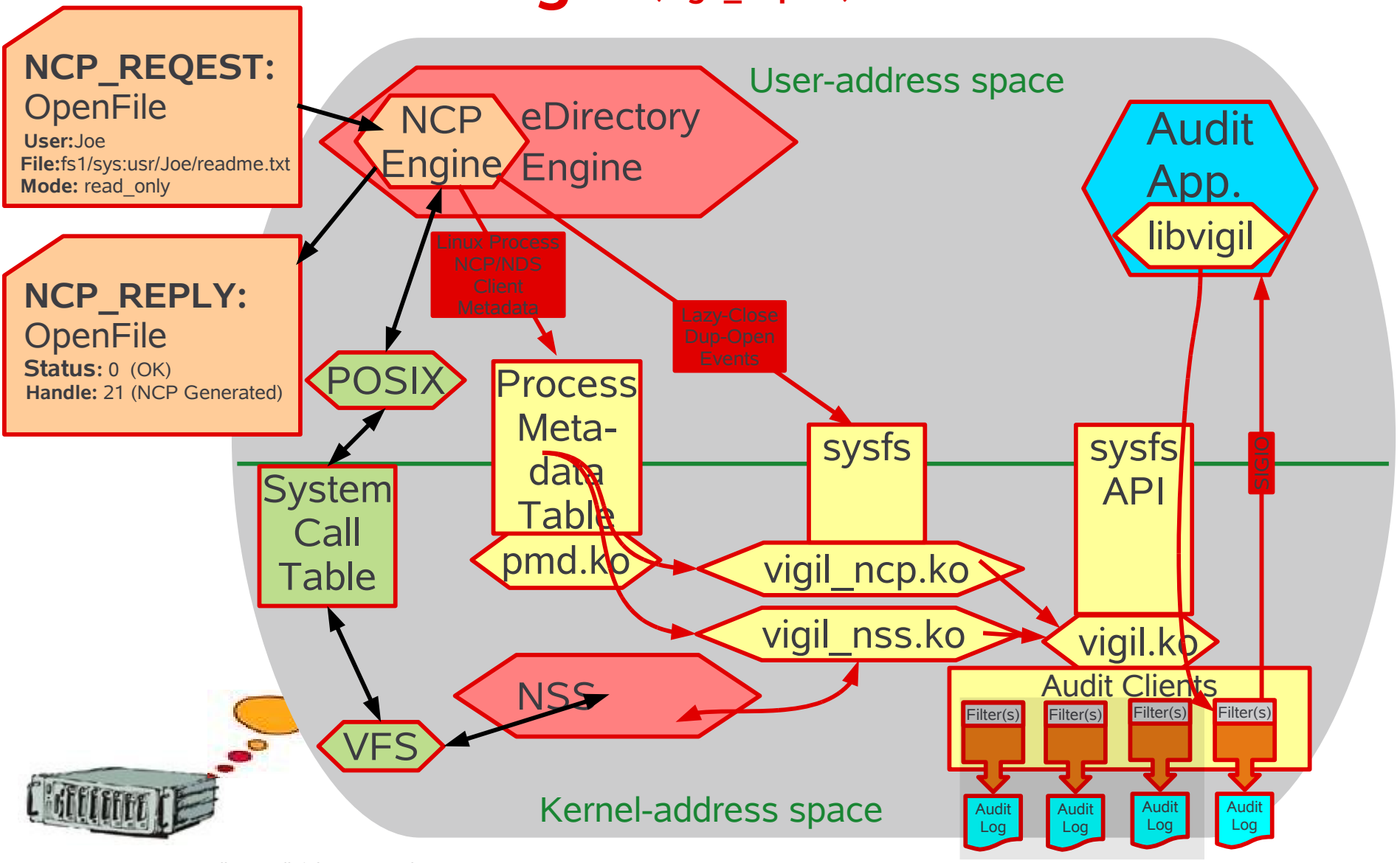
NCP Handling ...(Process Metadata Retrieval)



NCP Handling ...(Internal NCP Engine Event handling)

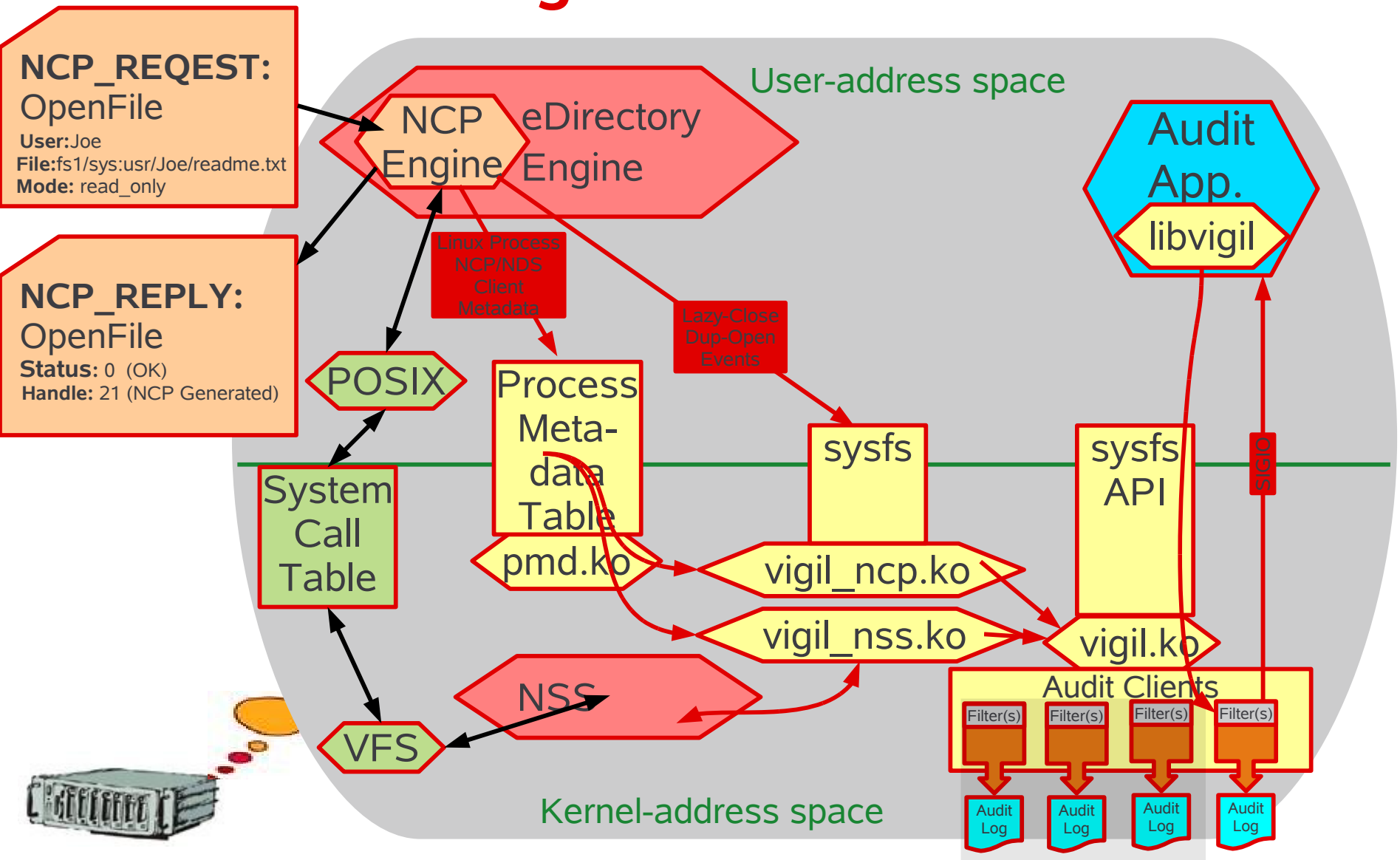


NCP Handling ...(vigil_ncp.ko)



CIFS, AFP, ...?

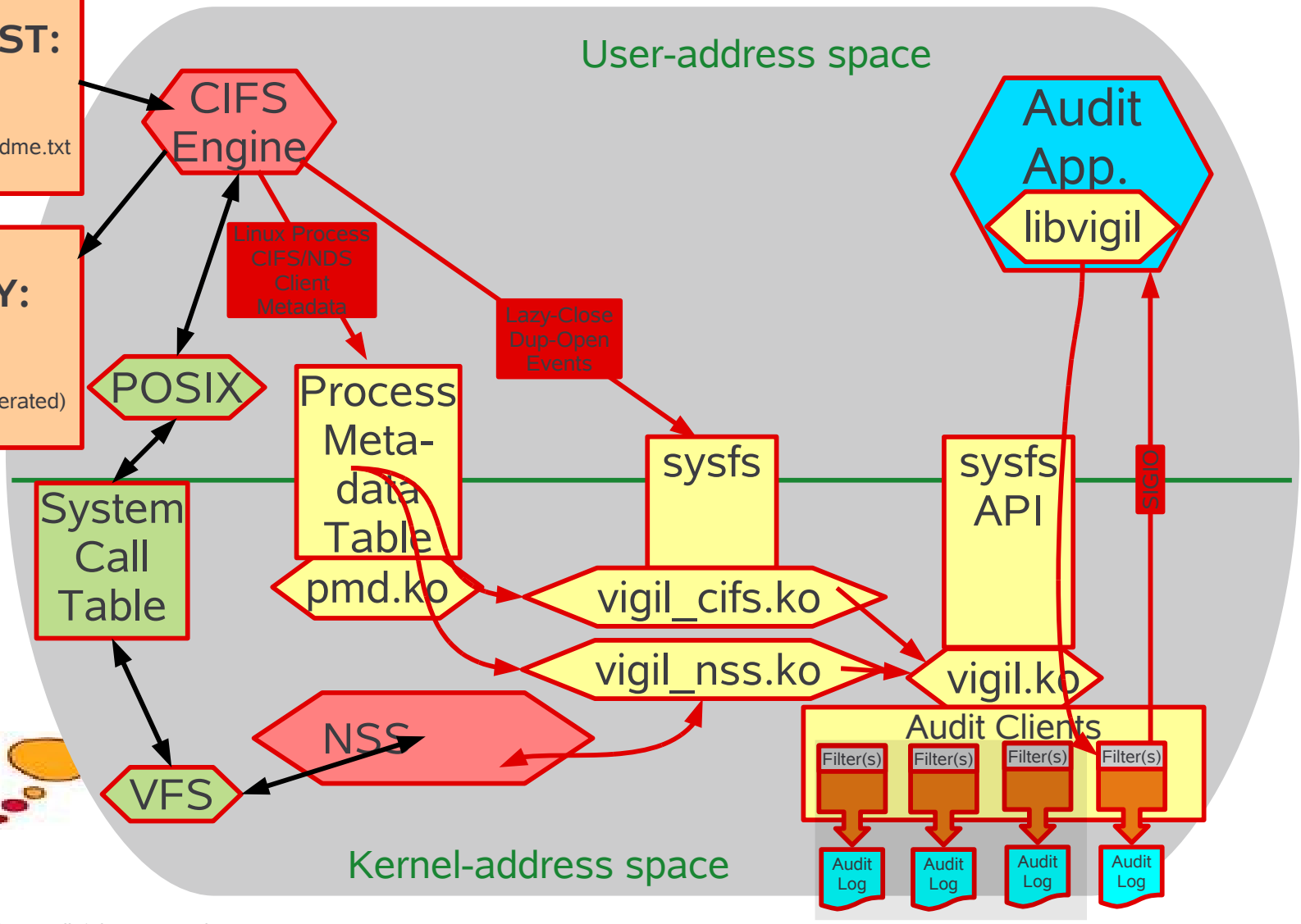
NCP Handling



CIFS Handling

CIFS_REQEST:
OpenFile
User: Joe
File:fs1/sys:usr/Joe/readme.txt
Mode: read_only

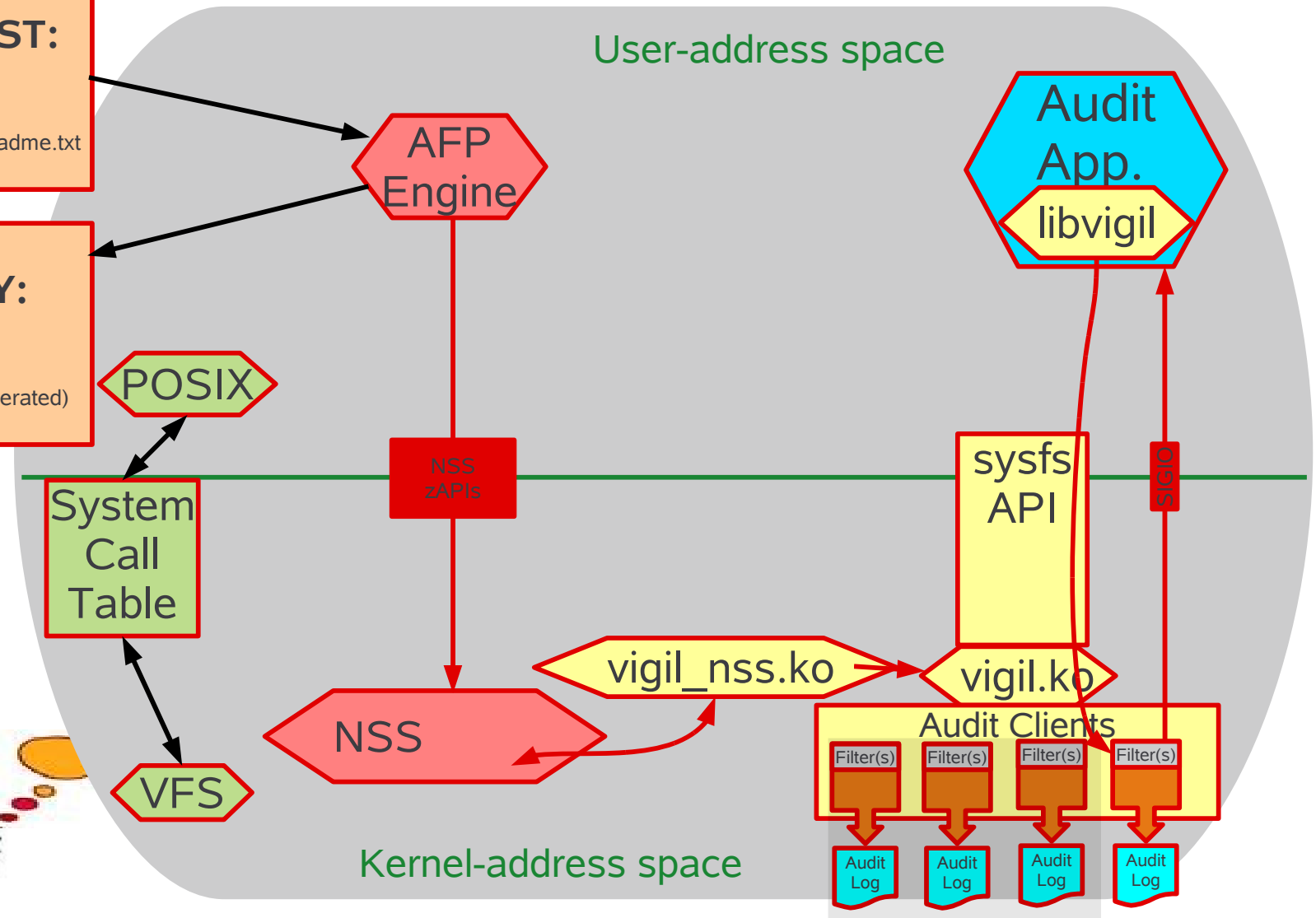
CIFS_REPLY:
OpenFile
Status: 0 (OK)
Handle: 21 (CIFS Generated)



AFP Handling

AFP_REQEST:
OpenFile
User: Joe
File:fs1/sys:usr/Joe/readme.txt
Mode: read_only

AFP_REPLY:
OpenFile
Status: 0 (OK)
Handle: 21 (AFP Generated)

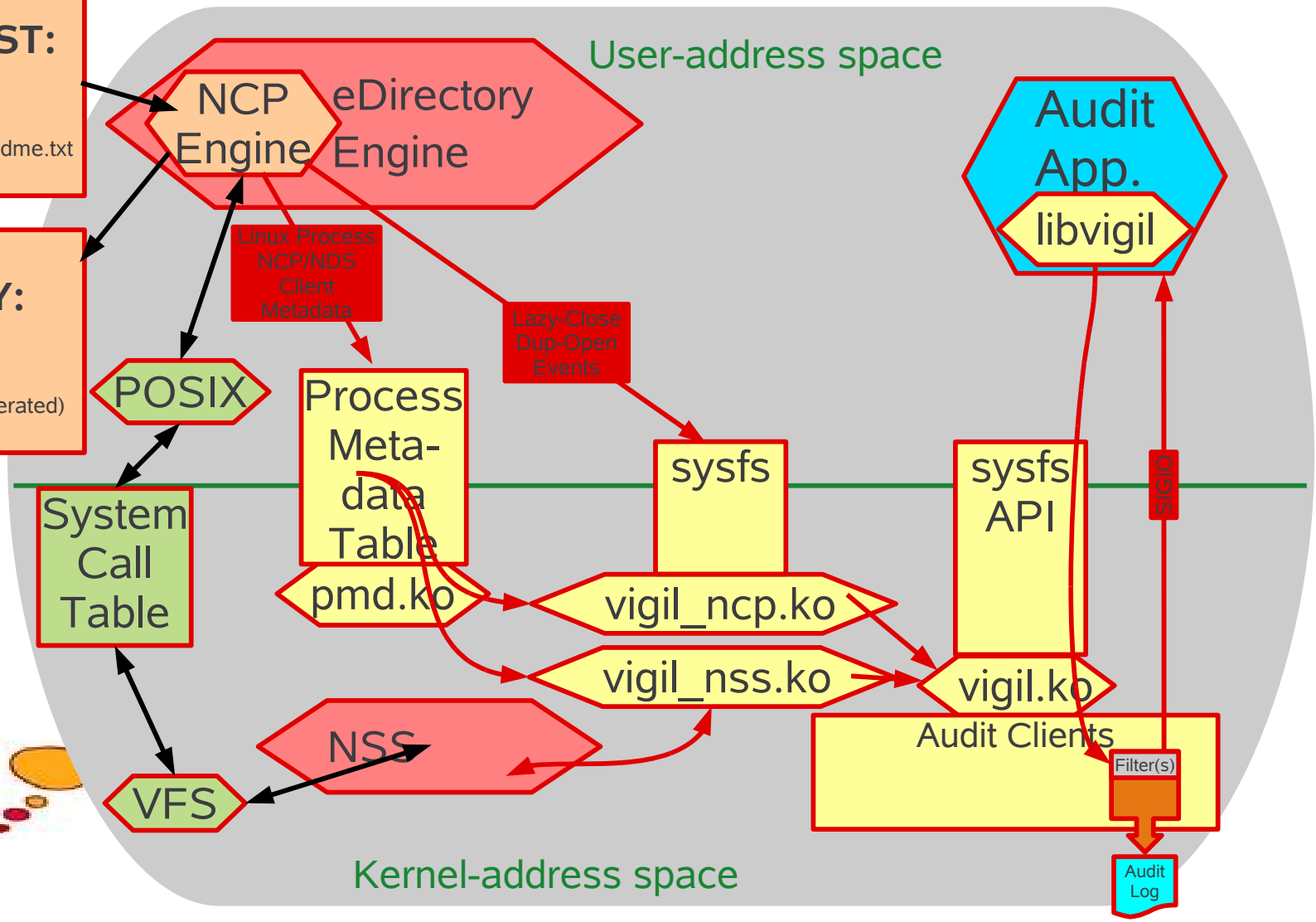


Audit Stream Filtering...

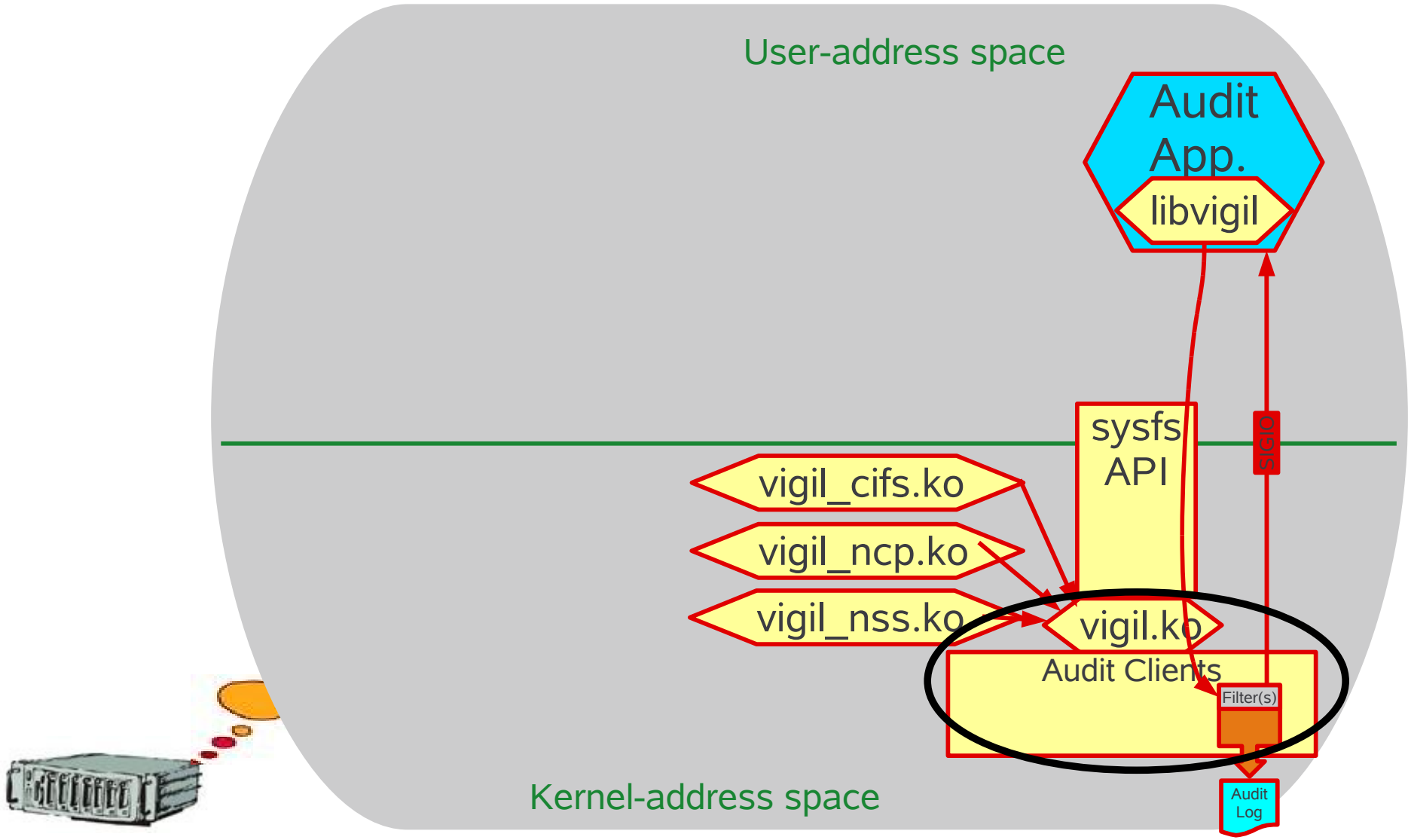
NCP Handling

NCP_REQEST:
OpenFile
User: Joe
File:fs1/sys:usr/Joe/readme.txt
Mode: read_only

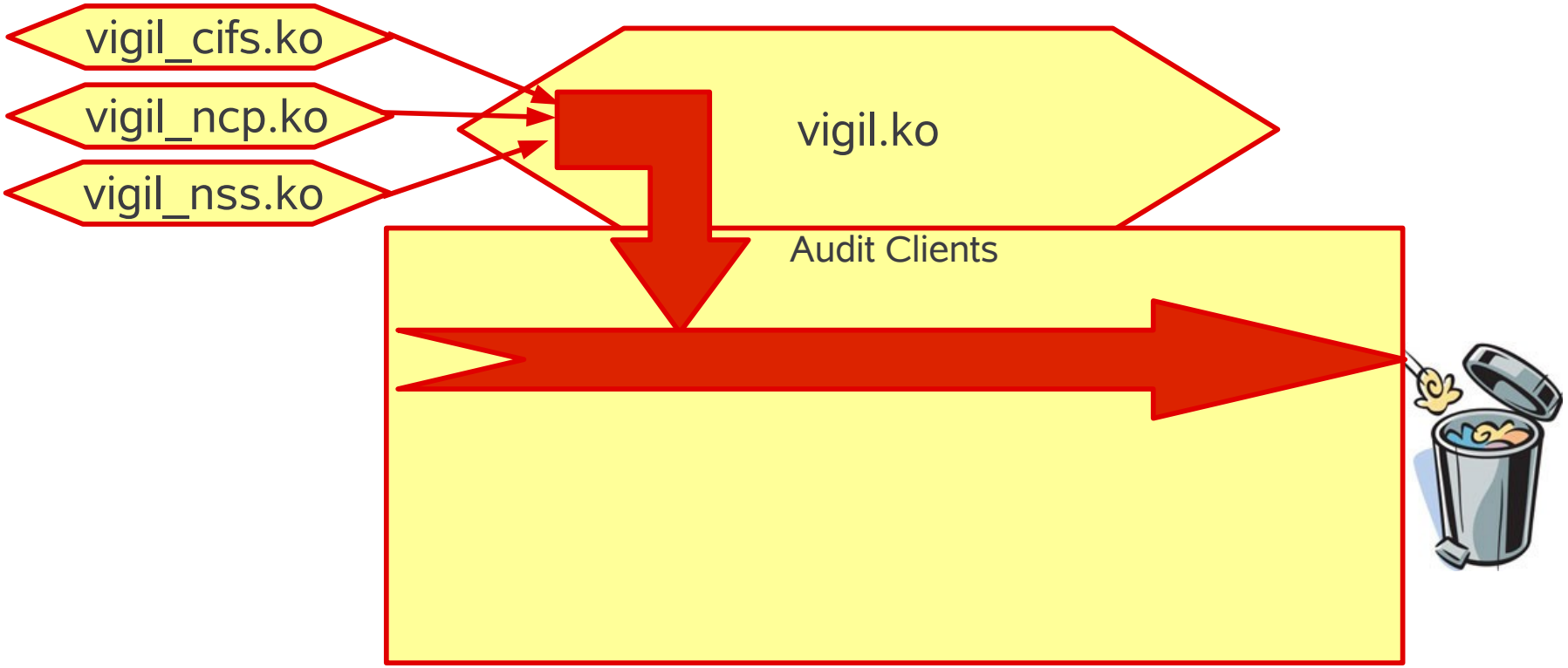
NCP_REPLY:
OpenFile
Status: 0 (OK)
Handle: 21 (NCP Generated)

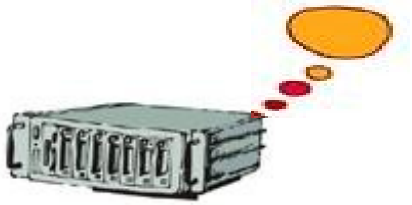


Auditing Client Filtering

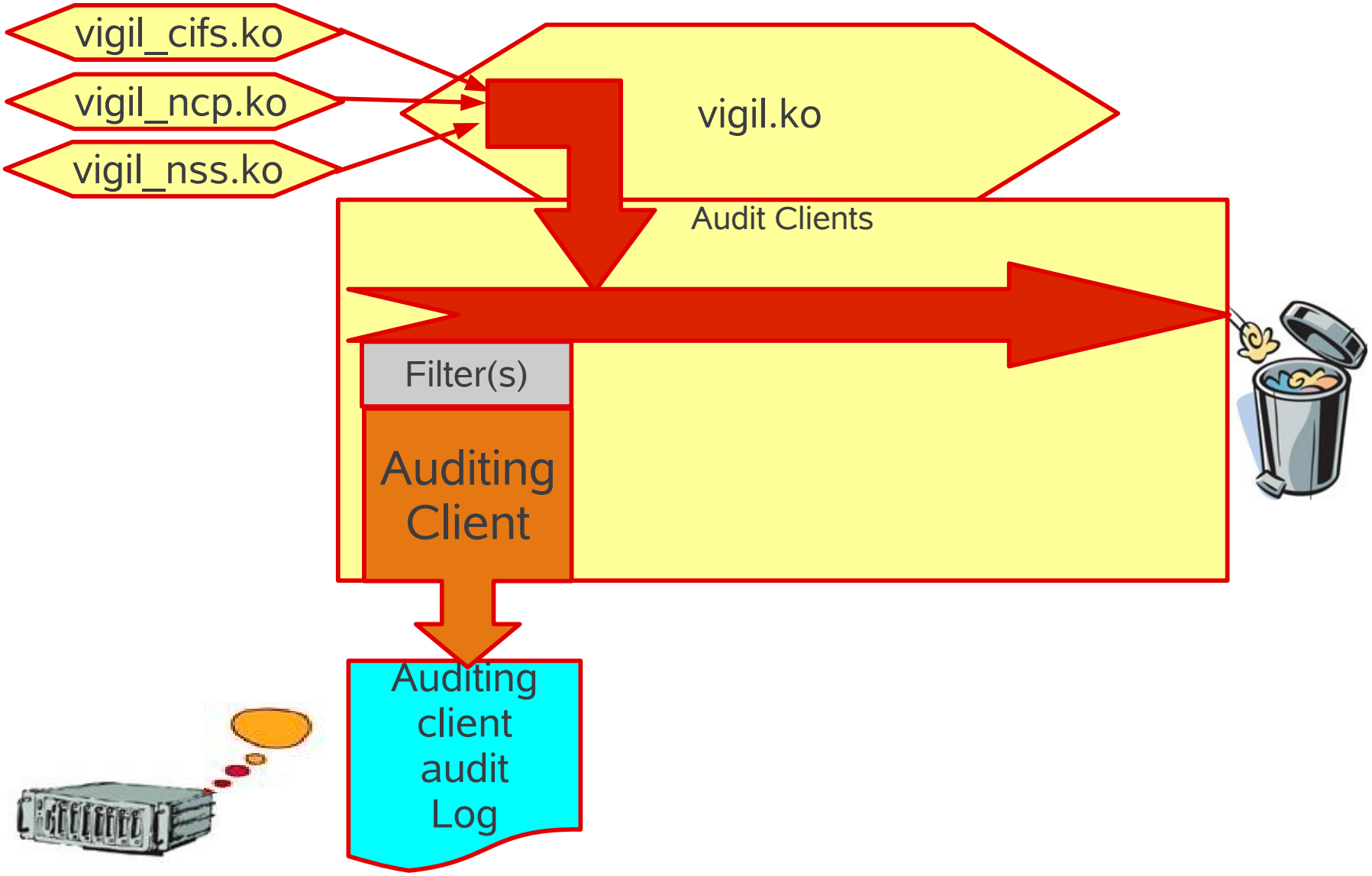


Filtering Internals ...(No Auditing Clients)

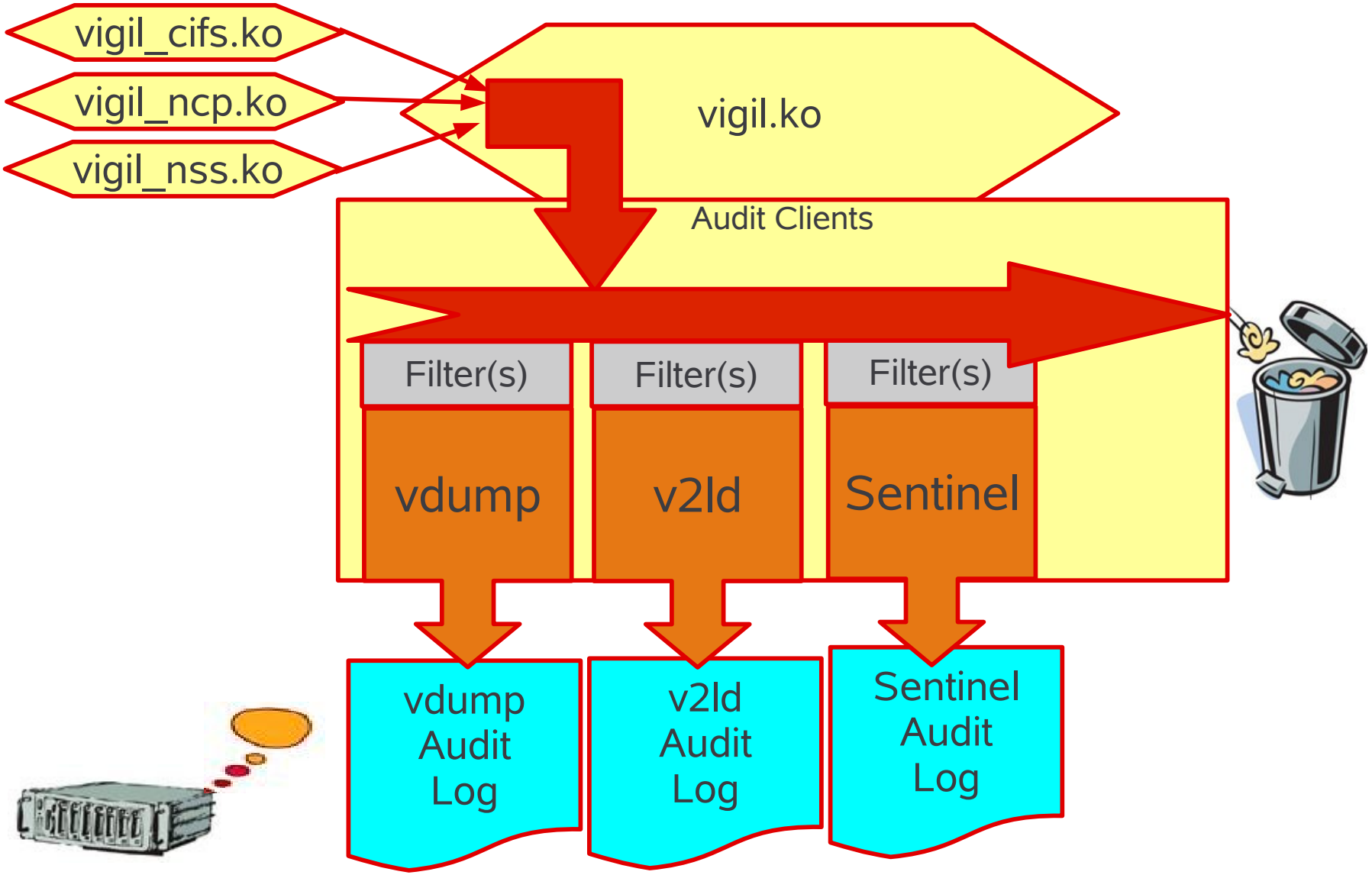




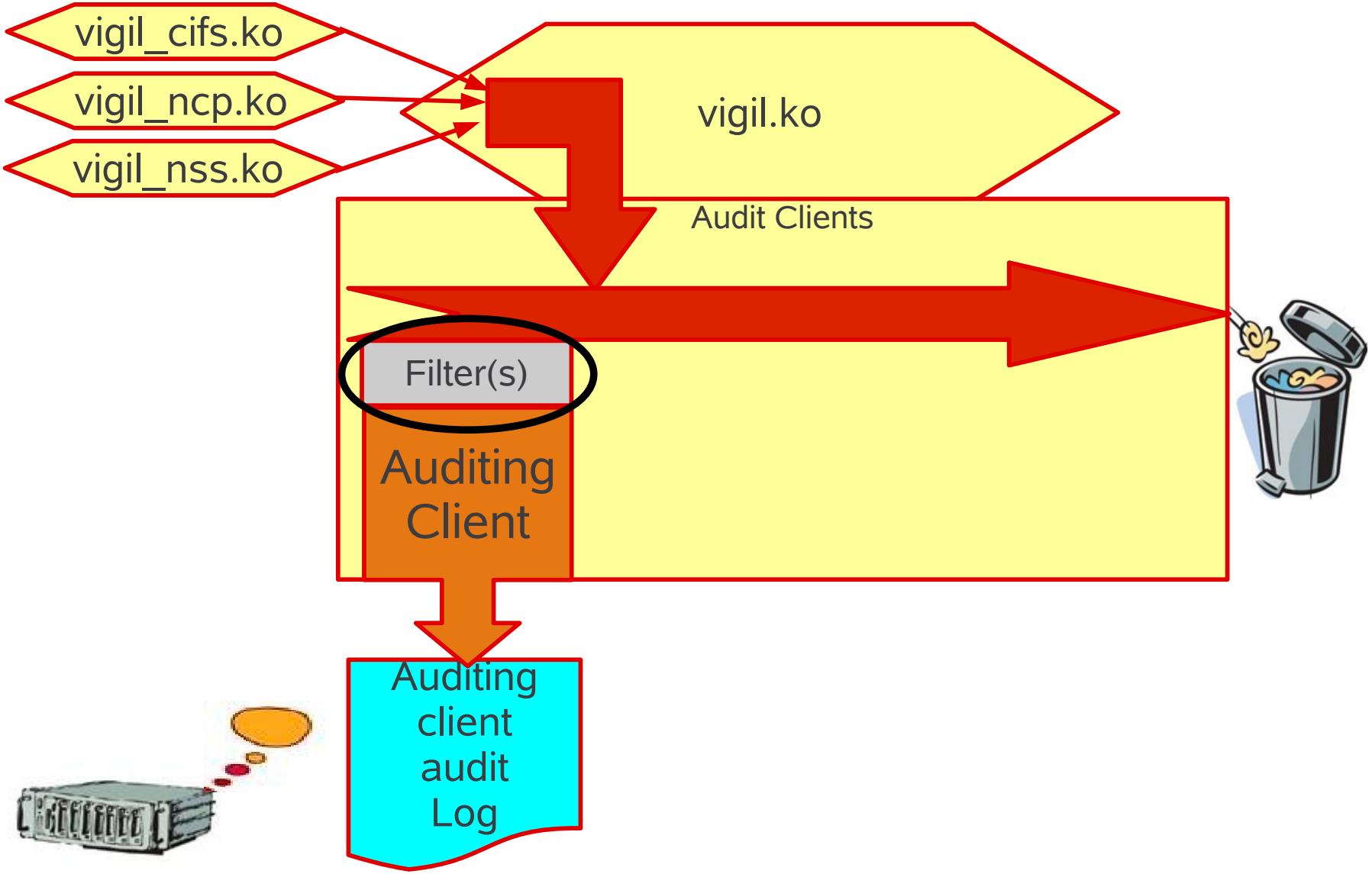
Filtering Internals ...(One Auditing Client)



Filtering Internals ...(Multiple Auditing Clients)



Filtering Internals ...(Filters)

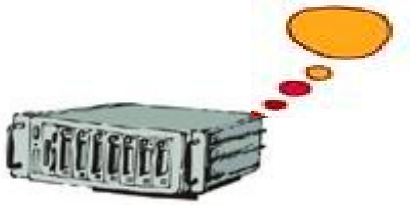


Filtering Internals ...(No filters, all events)

sign	length	type	recNo	pid	time	event
"/nvigil"	88	3	25	302	08/06/09 06:44 AM	4

FILTER(S):

Auditing Client



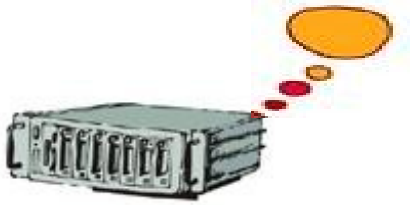
Filtering Internals ...(Filter types)

sign	length	type	recNo	pid	time	event
"/nvigil"	88	3	25	302	08/06/09 06:44 AM	4

FILTER(S):

Current filter types: Binary Include Filter, Binary Exclude Filter

Auditing Client



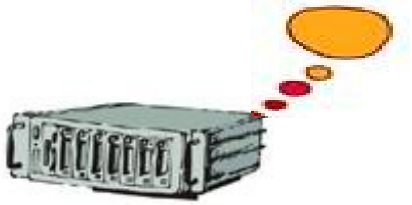
Filtering Internals ...(Include Filter)

sign	length	type	recNo	pid	time	event
"/nvigil"	88	3	25	302	08/06/09 06:44 AM	4
00001010...	01011000	00000011	00011001	0100101110	0000100000000110...	00000100 (OPEN)

FILTER(S):

F1 Include: 11

Auditing Client



Filtering Internals ...(Exclude Filters)

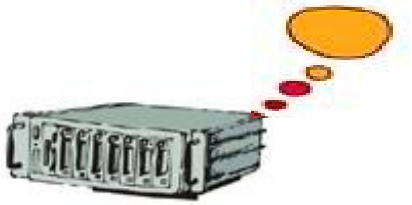
sign	length	type	recNo	pid	time	event
"/nvigil"	88	3	25	302	08/06/09 06:44 AM	4
00001010...	01011000	00000011	00011001	0100101110	0000100000000110...	00000100 (OPEN)

X

FR(S):

F1 Include: 11
F2 Exclude: 100101110

Auditing Client



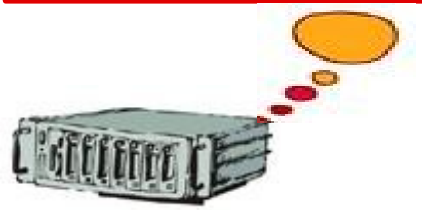
Filtering Internals ...(Combination Filters)

sign	length	type	recNo	pid	time	event
"/nvigil"	88	3	25	302	08/06/09 06:44 AM	4
00001010...	01011000	00000011	00011001	0100101110	0000100000000110...	00000100 (OPEN)

FILTER(S):

F1 Include:			11			
F2 Exclude:				100101110		
F3 Include:	1110110					
F4 Include:						100
F5 Exclude:					101	

Auditing Client



OES2/Linux -Fields in fixed length

Header fields:

- sign
- length
- type
- recNo
- pid
- time

Type “NSS” records:

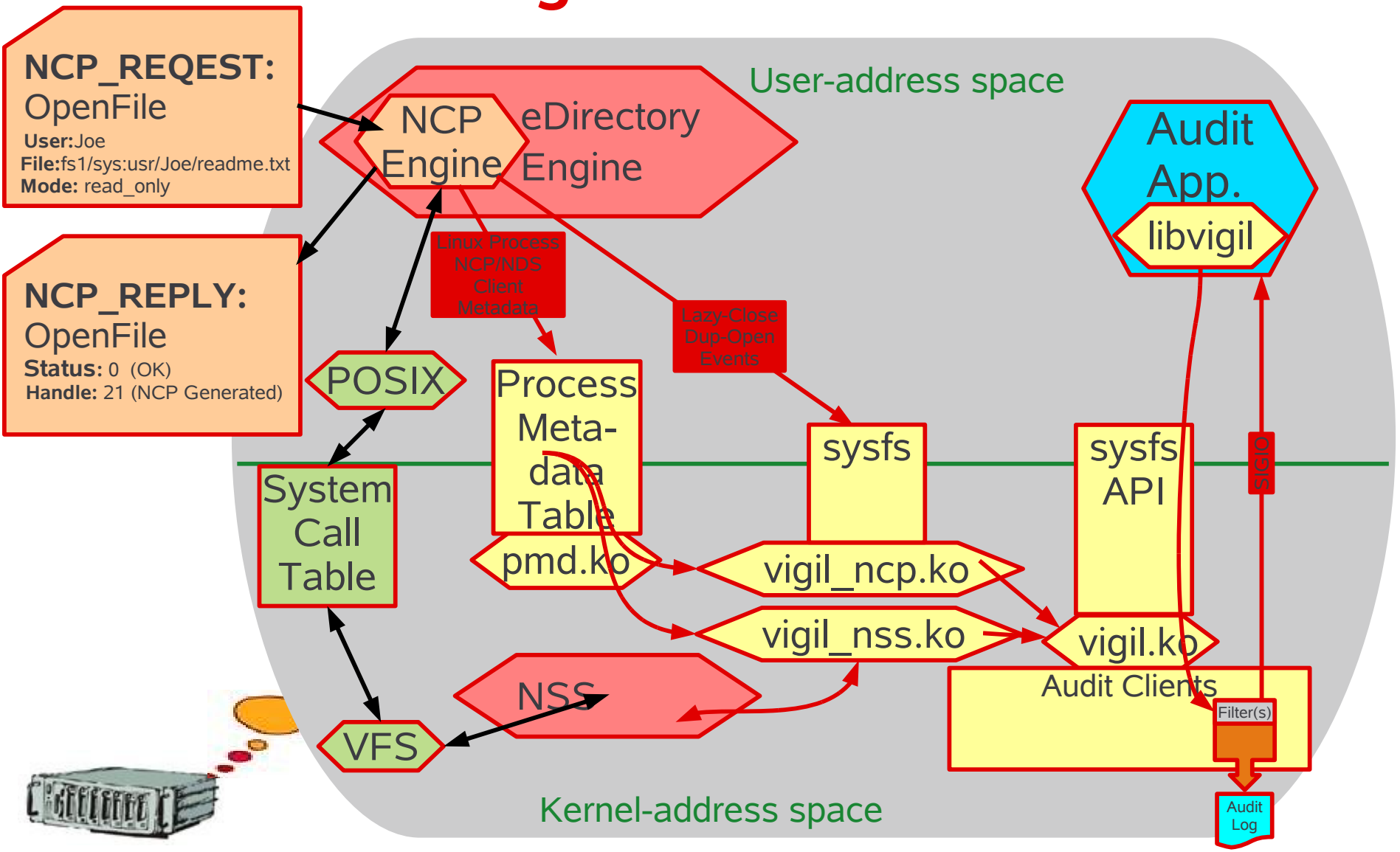
- event
- taskID
- volumeID
- zid
- parentZid
- userID
- fileType
- fileAttributes
- opRetCode
- uid
- guid
- comm

Type “vigil”, “ncp” and “cifs” records:

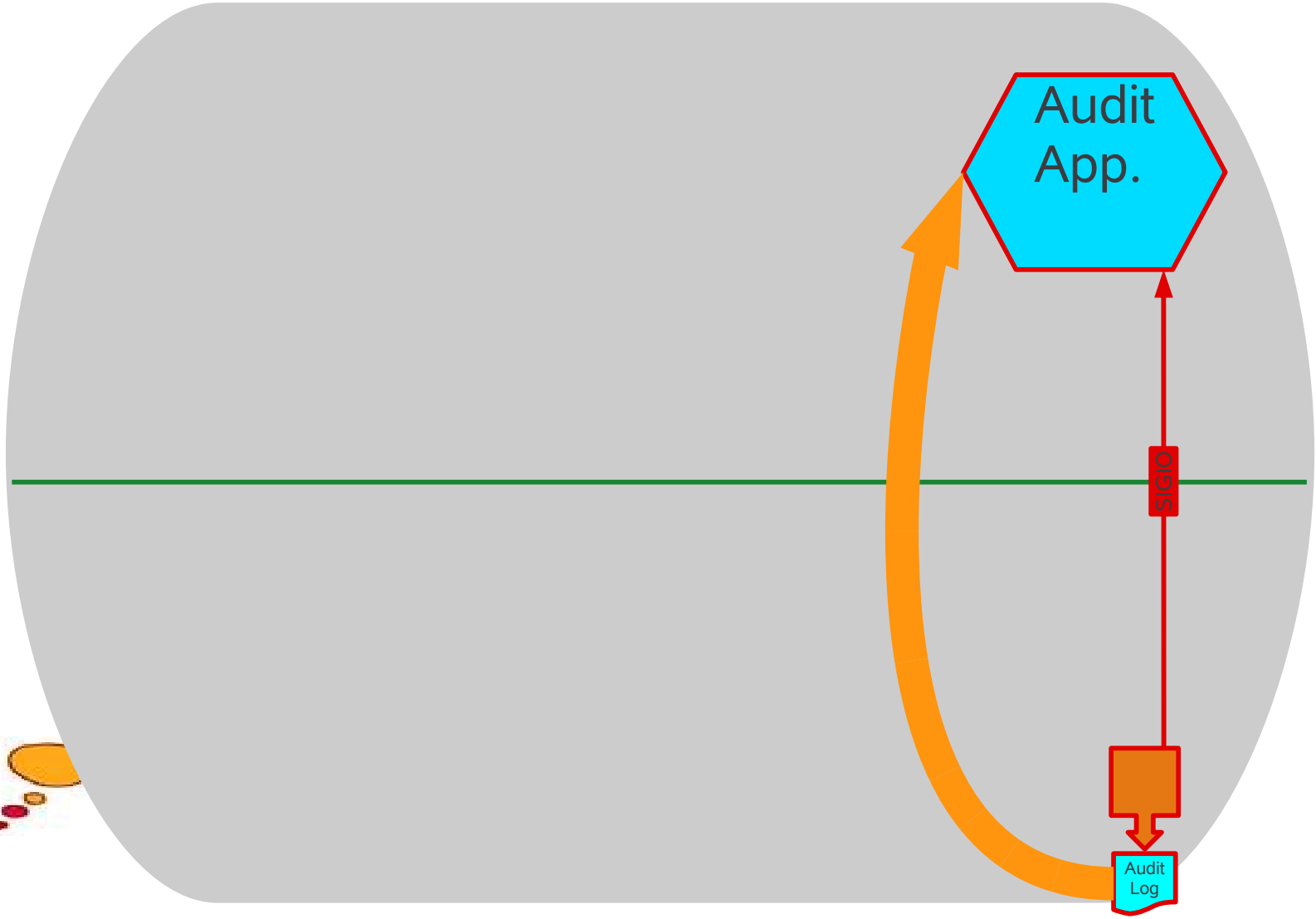
- event
- dataElements
- dataLength
- data

Audit Client Application Filtering

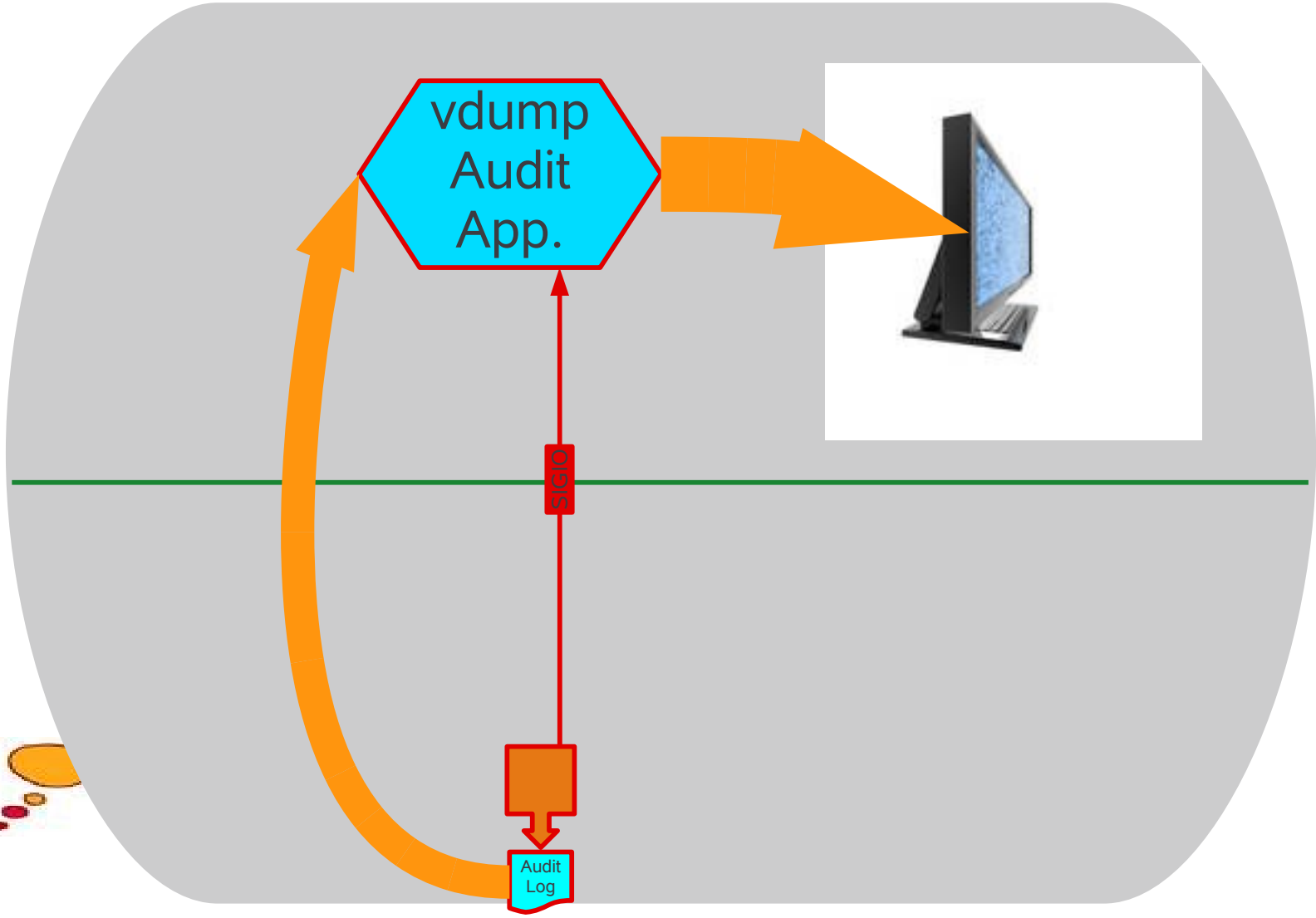
NCP Handling



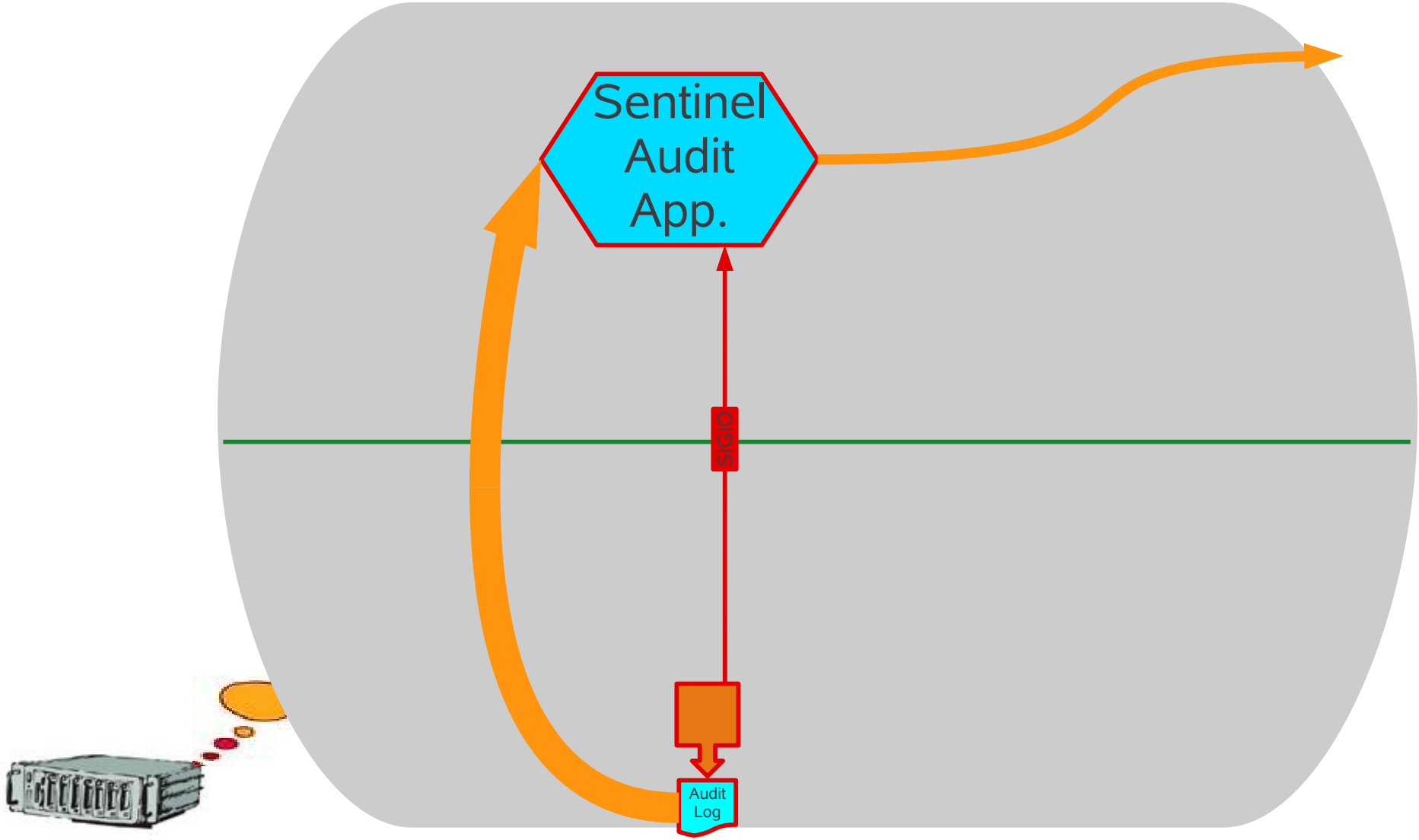
Application Filtering ...(The “Firehose”)



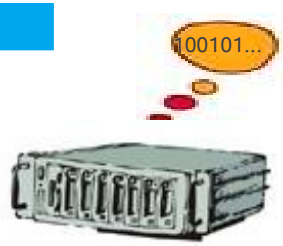
Application Filtering ...(vdump)

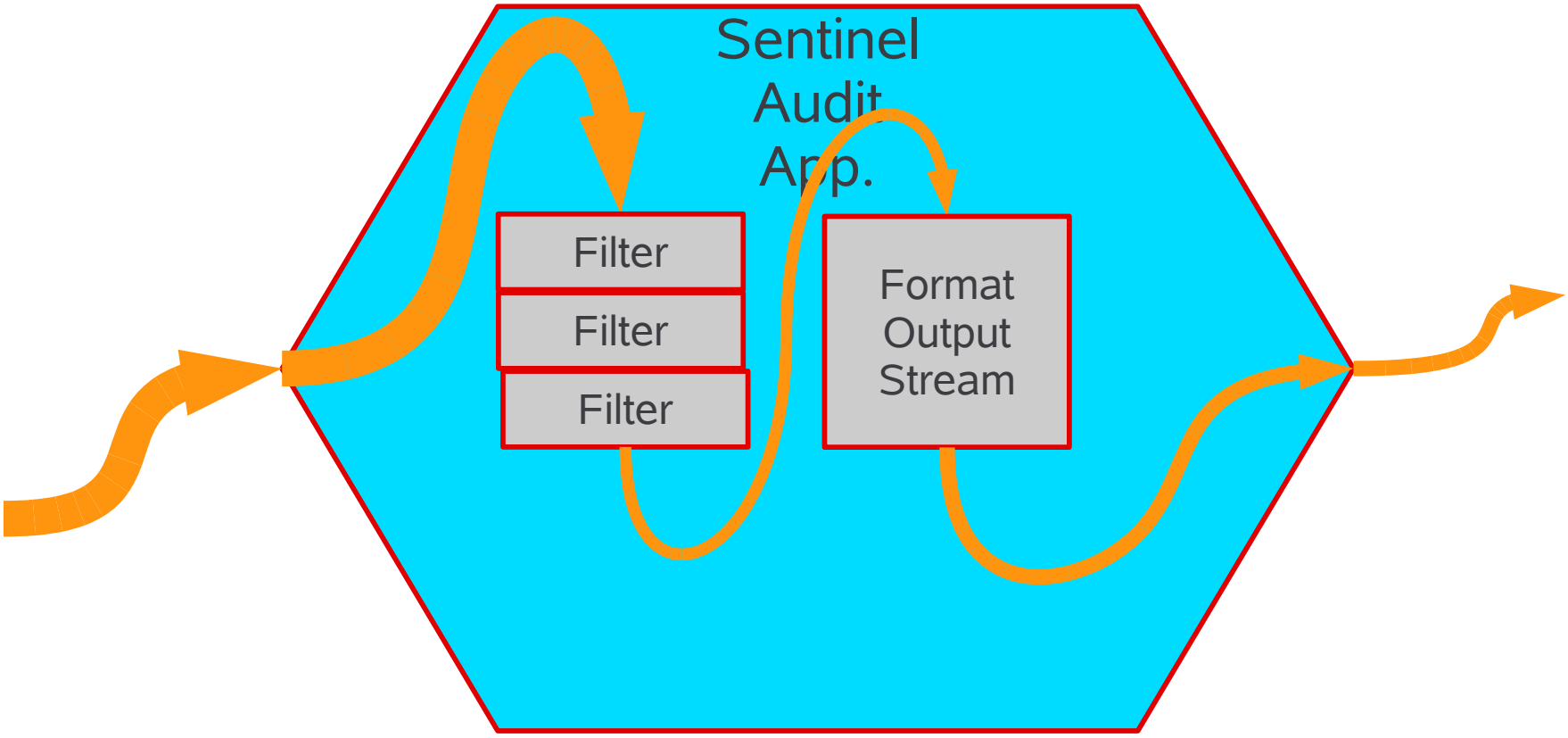


Application Filtering ...(Sentinel Auditing Client)



Application Filtering ...(Internals)





UNIT TWO

Linux OES2
Auditing Engine
Auditing Stream Structures

Audit Stream Structures - Overview

Audit Record Header

Record Types:

0 Vigil Records
2 NCP Records
3 NSS Records
4 CIFS Records

Record Element Types:

0x0002 VIGIL_ET_PATH
0x000C VIGIL_ET_MODIFY_zMOD_FILE_ATTRIBUTES
0x000D VIGIL_ET_MODIFY_zMOD_CREATED_TIME
0x000E VIGIL_ET_MODIFY_zMOD_ARCHIVED_TIME
0x000F VIGIL_ET_MODIFY_zMOD_MODIFIED_TIME
0x0010 VIGIL_ET_MODIFY_zMOD_ACCESSED_TIME
0x0011 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIED_TIME
0x0012 VIGIL_ET_MODIFY_zMOD_OWNER_ID
0x0013 VIGIL_ET_MODIFY_zMOD_ARCHIVER_ID
0x0014 VIGIL_ET_MODIFY_zMOD_MODIFIER_ID
0x0015 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIER_ID
0x0016 VIGIL_ET_MODIFY_zMOD_PRIMARY_NAMESPACE
0x0017 VIGIL_ET_MODIFY_zMOD_DELETED_INFO
0x0018 VIGIL_ET_MODIFY_zMOD_MAC_METADATA
0x0019 VIGIL_ET_MODIFY_zMOD_UNIX_METADATA
0x001A VIGIL_ET_MODIFY_zMOD_EXTATTR_FLAGS
0x001B VIGIL_ET_MODIFY_zMOD_VOL_ATTRIBUTES
0x001C VIGIL_ET_MODIFY_zMOD_VOL_NDS_OBJECT_ID
0x001D VIGIL_ET_MODIFY_zMOD_VOL_MIN_KEEP_SECONDS
0x001E VIGIL_ET_MODIFY_zMOD_VOL_MAX_KEEP_SECONDS
0x001F VIGIL_ET_MODIFY_zMOD_VOL_LOW_WATER_MARK
0x0020 VIGIL_ET_MODIFY_zMOD_VOL_HIGH_WATER_MARK
0x0021 VIGIL_ET_MODIFY_zMOD_POOL_ATTRIBUTES
0x0022 VIGIL_ET_MODIFY_zMOD_POOL_NDS_OBJECT_ID
0x0023 VIGIL_ET_MODIFY_zMOD_VOL_DATA_SHREDDING_COUNT
0x0024 VIGIL_ET_MODIFY_zMOD_VOL_QUOTA
0x0025 VIGIL_ET_MODIFY_zMOD_DIR_QUOTA
0x0026 VIGIL_ET_MODIFY_zMOD_READ_AHEAD_BLOCKS
0x0027 VIGIL_ET_MODIFY_zMOD_INH_RIGHTS_MASK
0x0028 VIGIL_ET_MODIFY_zMOD_ALL_TRUSTEES
0x0030 VIGIL_ET_WHO__LINUX
0x0034 VIGIL_ET_NAME
0x0035 VIGIL_ET_NCP_LOCAL_OPENFILE
0x0036 VIGIL_ET_NCP_LOCAL_CLOSEFILE
0x0038 VIGIL_ET_NSS_CREATE
0x0039 VIGIL_ET_NSS_OPEN
0x003A VIGIL_ET_NSS_CLOSE
0x003B VIGIL_ET_NSS_RENAME
0x003C VIGIL_ET_NSS_MODIFYINFO
0x003D VIGIL_ET_NSS_ADDTRUSTEE
0x003E VIGIL_ET_NSS_REMOVETRUSTEE
0x003F VIGIL_ET_NSS_SETINHERITEDRIGHTS
0x0040 VIGIL_ET_CIFS_LOCAL__OPENFILE
0x0041 VIGIL_ET_CIFS_LOCAL__CLOSEFILE
0x0042 VIGIL_ET_PMD_NCP
0x0043 VIGIL_ET_PMD_CIFS
0x0044 VIGIL_ET_NET_ADDR_IPv4
0x0045 VIGIL_ET_NET_ADDR_IPv6
0x0046 VIGIL_ET_NSS_LINK

Common Record Header

Common Header

Offset:	0 1 2 3 4 5	7 8 9 A	B C D E	F 10 11 12 13 14 15 16	17 18 19 1A	1B 1C 1D 1E	1F 20 21 22
Description:	sign	length	type	recNo	pid	time-secs	usecs

Element:	Type	Description
sign	5 Bytes	Start of record signature. [“\nVIGIL”]
length	uint32_t	Length of this audit record, including the header and all data elements.
type	uint32_t	Record type. (See table below)
recNo	uint64_t	Record number. This value is specific to the auditing client.
pid	uint32_t	Linux Process ID number which sponsored the event.
Time	timeval	Audit record timestamp, containing secs, and usecs sub-elements.

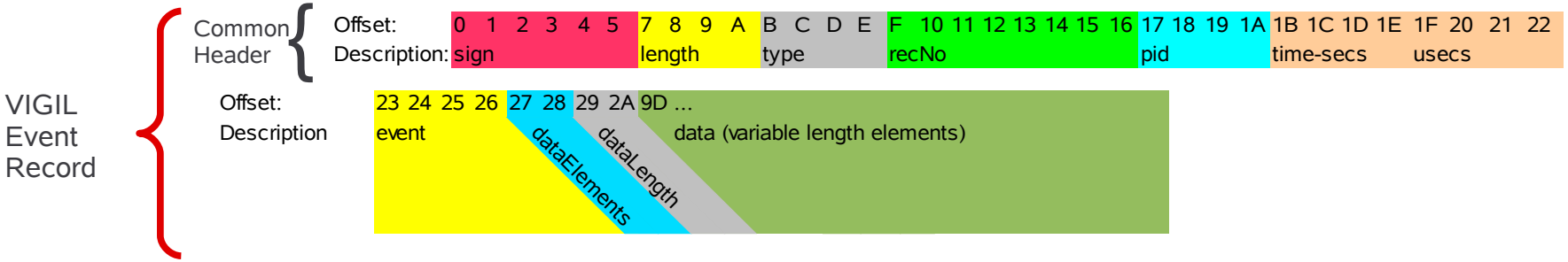
Event Types:

Value	Macro	Description
0	VIGIL_T_VIGIL	Internal audit engine event
2	VIGIL_T_NCP	NCP engine event.
3	VIGIL_T_NSS	NSS engine event.
4	VIGIL_T_CIFS	CIFS engine event.

Audit Records

Vigil (Audit Engine) Records
NCP Engine Records
CIFS Engine Records
NSS Engine Records

Audit File Records ...(VIGIL Event Record)

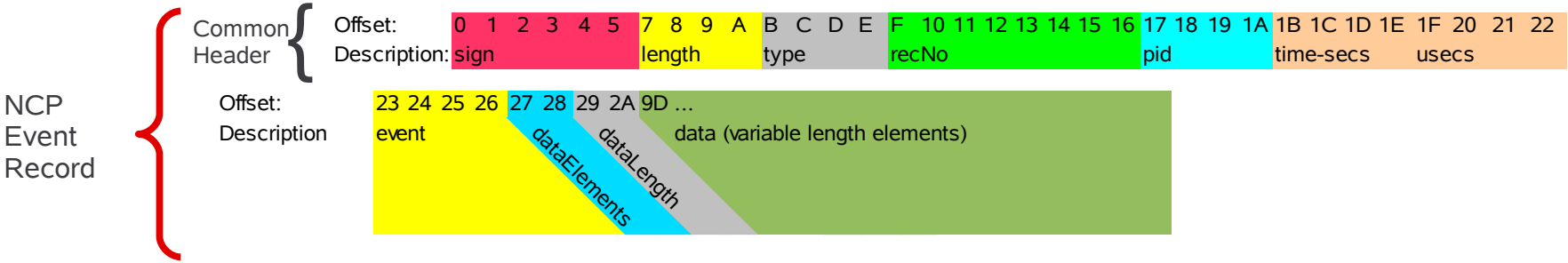


Element:	Type	Description
event	uint32_t	Event type (See table below)
dataElements	uint16_t	Number of data elements in the data area of the record.
dataLength	uint16_t	Length of the data area of the record (in bytes).
data		Contains 0 or more variable length data elements.

VIGIL Events:

Value	Macro	Description
·x·····۱	VIGIL_E_VIGIL_START	Auditing engine started. (vigil.ko)
·x·····۲	VIGIL_E_VIGIL_STOP	Auditing engine stopped.
·x····۱·	VIGIL_E_VIGIL_NCP_START	NCP auditing engine started (vigil_ncp.ko)
·x····۲·	VIGIL_E_VIGIL_NCP_STOP	NCP auditing engine stopped.
·x····۴·	VIGIL_E_VIGIL_CLIENT_START	Auditing client started.
·x····۸·	VIGIL_E_VIGIL_CLIENT_STOP	Auditing client stopped.
·x···۱··	VIGIL_E_VIGIL_USER_START	Auditing client user started.
·x···۲··	VIGIL_E_VIGIL_USER_STOP	Auditing client user stopped.
·x···۴··	VIGIL_E_VIGIL_ROLL	Audit log file full, rolling to new audit log file.
·x···۸··	VIGIL_E_VIGIL_NSS_START	NSS auditing engine started (vigil_nss.ko)
·x··۱···	VIGIL_E_VIGIL_NSS_STOP	NSS auditing engine stopped.
·x··۲···	VIGIL_E_VIGIL_CIFS_START	CIFS auditing engine started (vigil_cifs.ko)
·x··۴···	VIGIL_E_VIGIL_CIFS_STOP	CIFS auditing engine stopped.

Audit File Records ...(NCP Event Record)

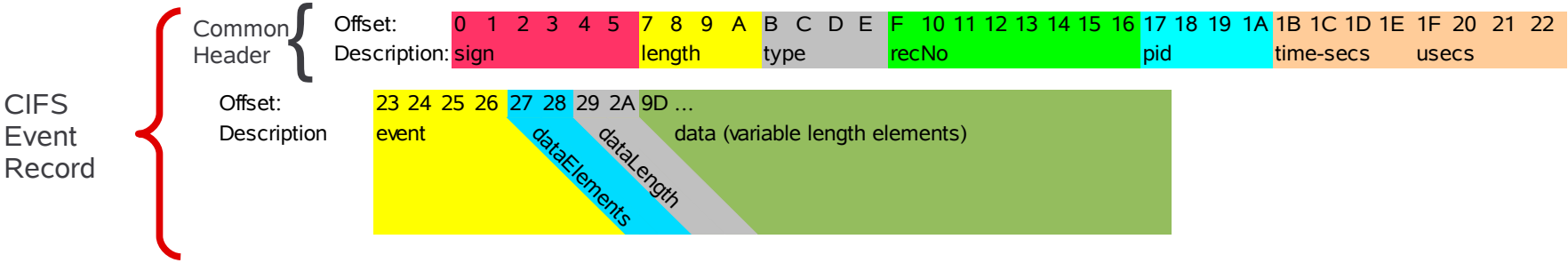


Element:	Type	Description
event	uint32_t	Event type (See table below)
dataElements	uint16_t	Number of data elements in the data area of the record.
dataLength	uint16_t	Length of the data area of the record (in bytes).
data		Contains 0 or more variable length data elements.

NCP Events:

Value	Macro	Description
0x00000010	VIGIL_E_NCP_OPEN	NCP Reporting that an NCP client has made an attempt to open a file.
0x00000020	VIGIL_E_NCP_CLOSE	NCP Reporting that an NCP client has made an attempt to close a file.

Audit File Records ...(CIFS Event Record)

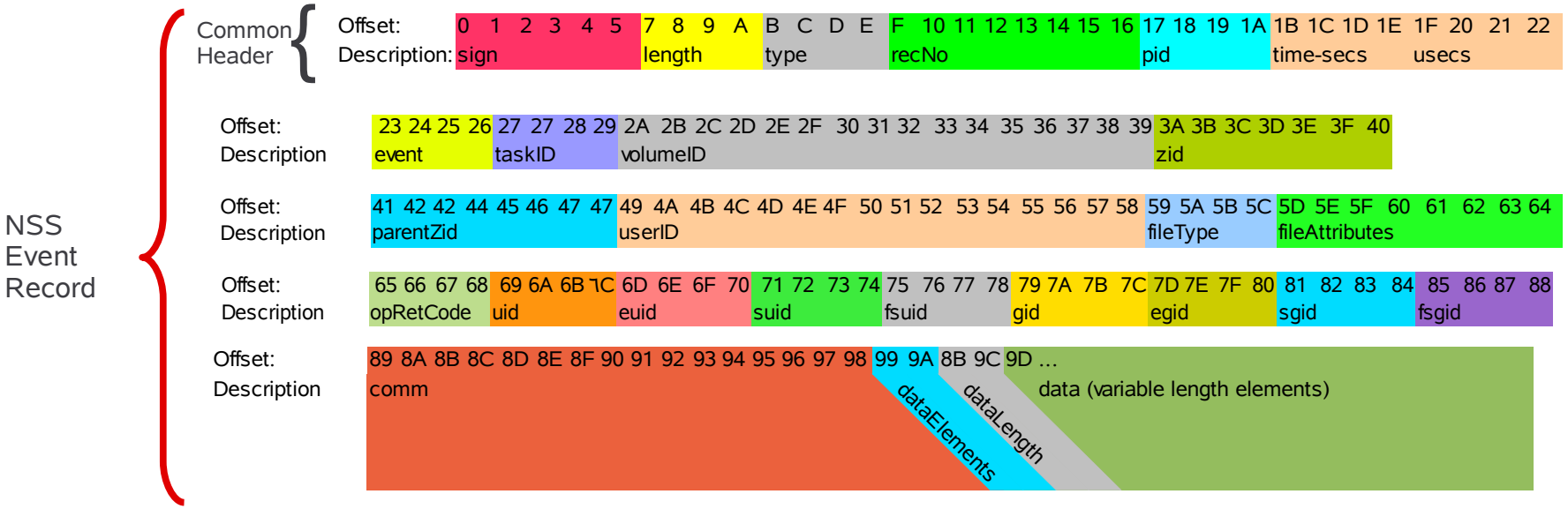


Element:	Type	Description
event	uint32_t	Event type (See table below)
dataElements	uint16_t	Number of data elements in the data area of the record.
dataLength	uint16_t	Length of the data area of the record (in bytes).
data		Contains 0 or more variable length data elements.

CIFS Events:

Value	Macro	Description
0x00000001	VIGIL_E_CIFS_OPEN	CIFS Reporting that a CIFS client has made an attempt to open a file.
0x00000002	VIGIL_E_CIFS_CLOSE	CIFS Reporting that an CIFS client has made an attempt to close a file.

Audit File Records ...(NSS Event Record)



Element:	Type	Description
event	uint32_t	Event type (See table below)
taskID	uint32_t	NCP/CIFS/AFP client taskID
volumeID	16 bytes	Volume (GUID) ID
zid	uint64_t	NSS object identifier number.
parentZid	uint64_t	NSS object identifier number of hierarchal parent object.
userID	16 bytes	eDir GUID of NCP/CIFS/AFP client, or NSS constant.
fileType	uint32_t	NSS object type (See table below).
fileAttributes	uint64_t	NSS object attributes (See table below).
opRetCode	uint32_t	NSS operation return code (0=Success. Nonzero=NSS error code.)
uid	uint32_t	Linux uid (user ID) of the process sponsoring this event.
euid	uint32_t	Linux “effective” uid of the process sponsoring this event.

Element:	Type	Description
suid	uint32_t	Linux “saved” uid of the process sponsoring this event.
fsuid	uint32_t	Linux “file system” uid of the process sponsoring this event.
gid	uint32_t	Linux gid (group ID) of the process sponsoring this event.
egid	uint32_t	Linux “effective” gid of the process sponsoring this event.
sgid	uint32_t	Linux “saved” gid of the process sponsoring this event.
fsgid	uint32_t	Linux “file system” gid of the process sponsoring this event.
comm	16 bytes	Name of user-space application that owns this process.
dataElements	uint16_t	Number of data elements in the data area of the record.
dataLength	uint16_t	Length of the data area of the record (in bytes).
data		Contains 0 or more variable length data elements.

NSS Events:

Value	Macro	Description
0x00000001	VIGIL_E_NSS_DELETE	NSS reporting that an object was deleted.
0x00000002	VIGIL_E_NSS_CREATE	NSS reporting that an object was created.
0x00000004	VIGIL_E_NSS_OPEN	NSS reporting that an object was opened.
0x00000008	VIGIL_E_NSS_CLOSE	NSS reporting that an object was closed.
0x00000010	VIGIL_E_NSS_RENAME	NSS reporting that an object was renamed.
0x00000020	VIGIL_E_NSS_LINK	NSS reporting that an object was linked.
0x00000040	VIGIL_E_NSS_MODIFY	NSS reporting that an object's metadata has been modified.
0x00000080	VIGIL_E_NSS_ADDTRUSTEE	NSS reporting that a trustee was added to this object.
0x00000100	VIGIL_E_NSS_REMOVETRUSTEE	NSS reporting that a trustee was removed from this object.
0x00000200	VIGIL_E_NSS_SETINHERITEDRIGHTS	NSS reporting that the inherited rights of this object has been set.

NSS Object Types:

Value	Macro	Description
0	zFILE_UNKNOWN	Unknown file type
1	zFILE_REGULAR	A file or directory
2	zFILE_EXTENDED_ATTRIBUTE	An extended attribute
3	zFILE_NAMED_DATA_STREAM	Resource forks for Mac OS
4	zFILE_PIPE	Unix style named pipe
5	zFILE_VOLUME	Logical storage
6	ZFILE_POOL	Physical storage

NSS Object Attributes:

Value	Macro	Value	Macro
0x00000001	zFA_READ_ONLY	0x00010000	zFA_IMMEDIATE_PURGE
0x00000002	zFA_HIDDEN	0x00020000	zFA_RENAME_INHIBIT
0x00000004	zFA_SYSTEM	0x00040000	zFA_DELETE_INHIBIT
0x00000008	zFA_EXECUTE	0x00080000	zFA_COPY_INHIBIT
0x00000010	zFA_SUBDIRECTORY	0x00100000	zFA_IS_ADMIN_LINK
0x00000020	zFA_ARCHIVE	0x00200000	zFA_IS_LINK
0x00000040	(UNDEFINED)	0x00400000	zFA_REMOTE_DATA_ACCESS
0x00000080	zFA_SHAREABLE	0x00800000	zFA_REMOTE_DATA_INHIBIT
0x00000100	(See “Search Mode Table”)	0x01000000	(UNDEFINED)
0x00000200	(See “Search Mode Table”)	0x02000000	zFA_COMPRESS_FILE_IMMEDIATELY
0x00000400	(See “Search Mode Table”)	0x04000000	zFA_DATA_STREAM_IS_COMPRESSED
0x00000800	zFA_NO_SUBALLOC	0x08000000	zFA_DO_NOT_COMPRESS_FILE
0x00001000	zFA_TRANSACTION	0x10000000	zFA_HARDLINK
0x00002000	zFA_NOT_VIRTUAL_FILE	0x20000000	zFA_CANT_COMPRESS_DATA_STREAM
0x00004000	(UNDEFINED)	0x40000000	zFA_ATTR_ARCHIVE
0x00008000	(UNDEFINED)	0x80000000	zFA_VOLATILE

Search Mode Table

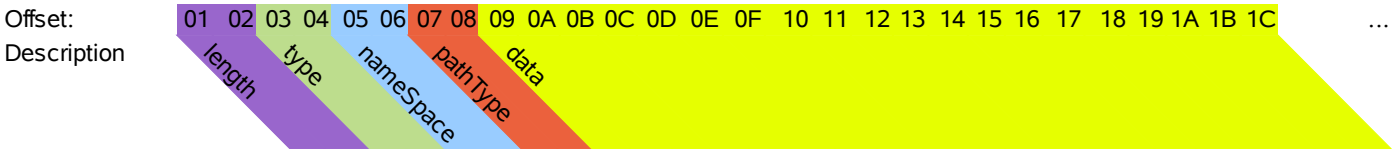
zFA_SMODE_BITS:

0x00000400	0x00000200	0x00000100	Value	Search Mode
0	0	0	0	Search on all read only opens
0	0	1	1	Search on read only opens with no path
0	1	0	2	Shell default search mode
0	1	1	3	Search on all opens with no path
1	0	0	4	Do not search
1	0	1	5	(Reserved)
1	1	0	6	Search on all opens with no path
1	1	1	7	(Reserved)

OES2/Linux/Auditing

Audit File Record Elements...

0x0002 VIGIL_ET_PATH (VIGIL_ELEMENT_PATH_T)



Element:	Type	Description
length	uint16_t	Length of element (in bytes).
type	uint16_t	0x0002 VIGIL_ET_PATH
nameSpace	uint16_t	(See table below)
pathType	uint16_t	(See table below)
data		Path value

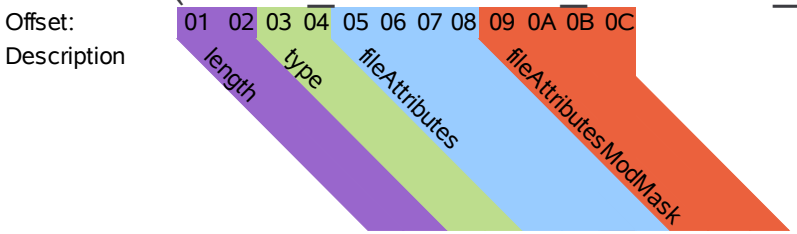
nameSpace values:

Value	Macro	Description
0x0000	VIGIL_ELEMENT_PATH_NS_ANONYMOUS	Unknown nameSpace
0x0001	VIGIL_ELEMENT_PATH_NS_FAMILIAR	ASCII path.
0x0002	VIGIL_ELEMENT_PATH_NS_UNICODE	Unicode path

pathType values:

Value	Macro	Description
0x0000	VIGIL_ELEMENT_PATH_TYPE_ANONYMOUS	Unknown pathType.
0x0001	VIGIL_ELEMENT_PATH_TYPE_TARGET	Path represents a target of open, create, delete, etc.
0x0002	VIGIL_ELEMENT_PATH_TYPE_SOURCE	Path represents a (move) source path
0x0003	VIGIL_ELEMENT_PATH_TYPE_DESTINATION	Path represents a (move) destination path

0x000C VIGIL_ET_MODIFY_zMOD_FILE_ATTRIBUTES (VIGIL_ELEMENT_MODIFY__zMOD_FILE_ATTRIBUTES_T)



length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x000C VIGIL_ET_MODIFY_zMOD_FILE_ATTRIBUTES
fileAttributes	uint32_t	Bit attributes (See table below)
fileAttributesModMask	uint32_t	Applicable bits (modified by this operation).

fileAttribute bit values:

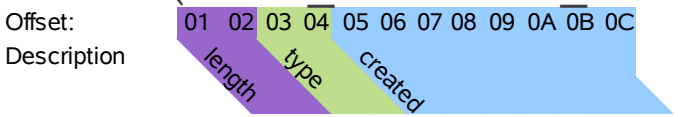
0x00000008	zFA_EXECUTE	File can be loaded for execution only. Once set, cannot be cleared.
0x00000010	zFA_SUBDIRECTORY	Entry is a subdirectory, not a file.
0x00000020	zFA_ARCHIVE	(file) has been modified since last archive or backup.
0x00000040	(deprecated)	(deprecated) Execute confirm.
0x00000080	zFA_SHAREABLE	Object can be simultaneously accessed by more than one user.
0x00000100	zFA_SMODE_BITS [1]	(See Search Mode table below)
0x00000200	zFA_SMODE_BITS [2]	(See Search Mode table below)
0x00000400	zFA_SMODE_BITS [3]	(See Search Mode table below)
0x00000800	zFA_NO_SUBALLOC	Disables block suballocation. (Larger file footprint, frequently changing files)
0x00001000	zFA_TRANSACTION	Transaction Tracking Services (TTS) enabled
0x00002000	zFA_NOT_VIRTUAL_FILE	Only valid on volumes with zATTR_VIRTUAL_FILES attribute set
0x00004000	(Unused) zFA_ReadAudit	Only settable by user with supervisor security equivalence.
0x00008000	(Unused) zFA_WriteAudit	Only settable by user with supervisor security equivalence.
0x00010000	zFA_IMMEDIATE_PURGE	File may not be undeleted after it is deleted.
0x00020000	zFA_RENAME_INHIBIT	Rename operation not allowed
0x00040000	zFA_DELETE_INHIBIT	Delete operation not allowed
0x00080000	zFA_COPY_INHIBIT	Copy operation not allowed (only works with MACs)
0x00100000	zFA_IS_ADMIN_LINK	File contains persistent admin link info. (Old auditing bit).
0x00200000	zFA_IS_LINK	
0x00400000	zFA_REMOTE_DATA_ACCESS	File has been migrated. (to tape, or other alternative storage)
0x00800000	zFA_REMOTE_DATA_INHIBIT	Don't allow file migration.(to tape, or other alternative storage)
0x01000000	(unused)	(Old Data Micragion Save Key Bit)
0x02000000	zFA_COMPRESS_FILE_IMMEDIATELY	File is compressed immediately (when closed).
0x04000000	zFA_DATA_STREAM_IS_COMPRESSED	Per data stream directory entry.
0x08000000	zFA_DO_NOT_COMPRESS_FILE	Prevents NSS from ever compressing the file.
0x10000000	zFA_HARD_LINK	Hardlink NSS object. Real inode is pointed to by FILE
0x20000000	zFA_CANT_COMPRESS_DATA_STREAM	Can't save any space by compressing this data stream
0x40000000	zFA_ATTR_ARCHIVE	
0x80000000	zFA_VOLATILE	Data is volatile (no oplocks)

Search Mode Table

zFA_SMODE_BITS:

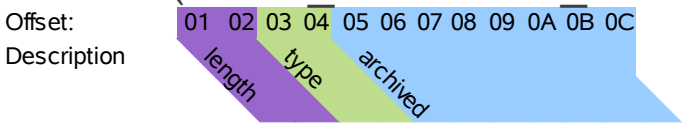
0x00000400	0x00000200	0x00000100	Value	Search Mode
0	0	0	0	Search on all read only opens
0	0	1	1	Search on read only opens with no path
0	1	0	2	Shell default search mode
0	1	1	3	Search on all opens with no path
1	0	0	4	Do not search
1	0	1	5	(Reserved)
1	1	0	6	Search on all opens with no path
1	1	1	7	(Reserved)

0x000D VIGIL_ET_MODIFY_zMOD_CREATED_TIME (VIGIL_ELEMENT_MODIFY__zMOD_CREATED_TIME_T)



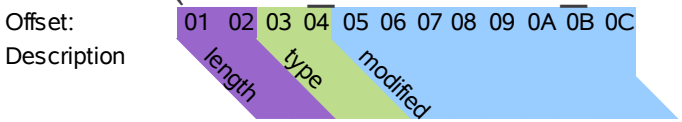
Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x000D VIGIL_ET_MODIFY_zMOD_CREATED_TIME
created	uint64_t	“struct timeval” representation of the date and time that this NSS object was created.

0x000E VIGIL_ET_MODIFY_zMOD_ARCHIVED_TIME (VIGIL_ELEMENT_MODIFY__zMOD_ARCHIVED_TIME_T)



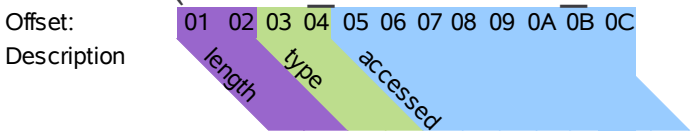
Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x000E VIGIL_ET_MODIFY_zMOD_ARCHIVED_TIME
archived	uint64_t	“struct timeval” representation of the date and time that this NSS object was last archived.

0x000F VIGIL_ET_MODIFY_zMOD_MODIFIED_TIME (VIGIL_ELEMENT_MODIFY__zMOD_MODIFIED_TIME_T)



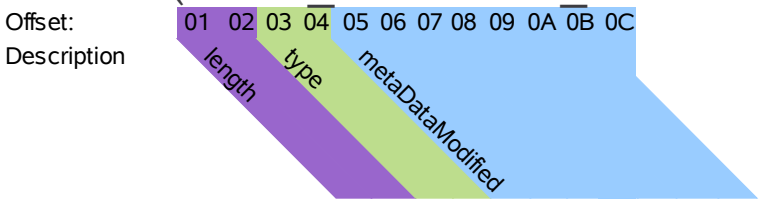
Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x000F VIGIL_ET_MODIFY_zMOD_MODIFIED_TIME
modified	uint64_t	“struct timeval” representation of the date and time that this NSS object was last modified.

0x0010 VIGIL_ET_MODIFY_zMOD_ACCESSED_TIME (VIGIL_ELEMENT_MODIFY__zMOD_ACCESSED_TIME_T)



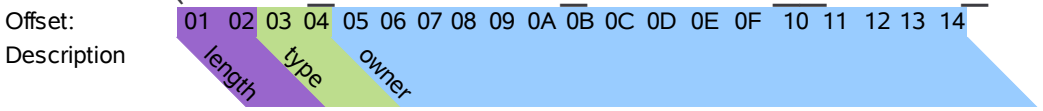
Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x0010 VIGIL_ET_MODIFY_zMOD_ACCESSED_TIME
accessed	uint64_t	“struct timeval” representation of the date and time that this NSS object was last accessed.

0x0011 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIED_TIME (VIGIL_ELEMENT_MODIFY__zMOD_METADATA_MODIFIED_TIME_T)



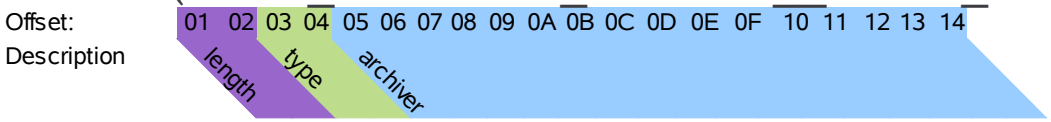
Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x0011 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIED_TIME
metaDataModified	uint64_t	“struct timeval” representation of the date and time that this NSS object's metadata was last modified.

0x0012 VIGIL_ET_MODIFY_zMOD_OWNER_ID (VIGIL_ELEMENT_MODIFY__zMOD_OWNER_ID_T)



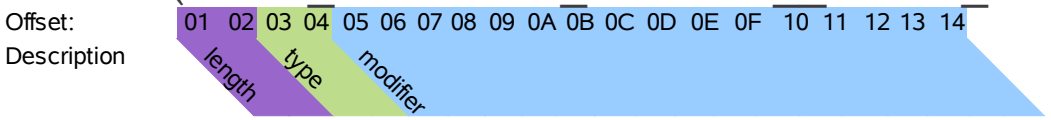
Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0012 VIGIL_ET_MODIFY_zMOD_OWNER_ID
owner	16 Bytes	eDir GUID of the owner of this NSS object.

0x0013 VIGIL_ET_MODIFY_zMOD_ARCHIVER_ID (VIGIL_ELEMENT_MODIFY__zMOD_ARCHIVER_ID_T)



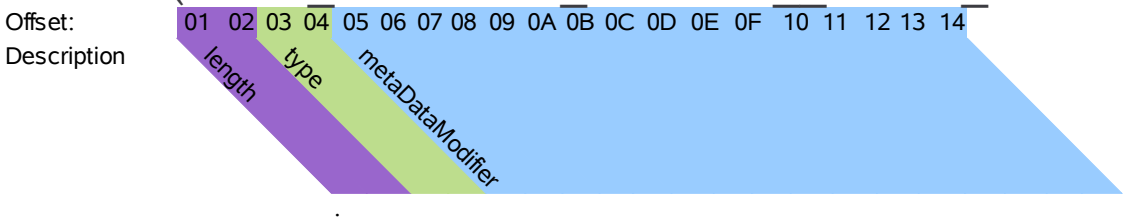
Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0013 VIGIL_ET_MODIFY_zMOD_ARCHIVER_ID
archiver	16 Bytes	eDir GUID of the last archiver of this NSS object.

0x0014 VIGIL_ET_MODIFY_zMOD_MODIFIER_ID (VIGIL_ELEMENT_MODIFY__zMOD_MODIFIER_ID_T)



Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0014 VIGIL_ET_MODIFY_zMOD_MODIFIER_ID
modifier	16 Bytes	eDir GUID of the last modifier of this NSS object.

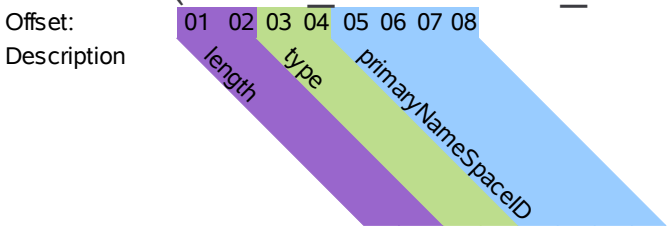
0x0015 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIER_ID (VIGIL_ELEMENT_MODIFY__zMOD_METADATA_MODIFIER_ID_T)



.

Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0015 VIGIL_ET_MODIFY_zMOD_METADATA_MODIFIER_ID
metaDataModifier	16 Bytes	eDir GUID of the last metadata modifier of this NSS object.

0x0016 VIGIL_ET_MODIFY_zMOD_PRIMARY_NAMESPACE (VIGIL_ELEMENT_MODIFY__zMOD_PRIMARY_NAMESPACE_T)

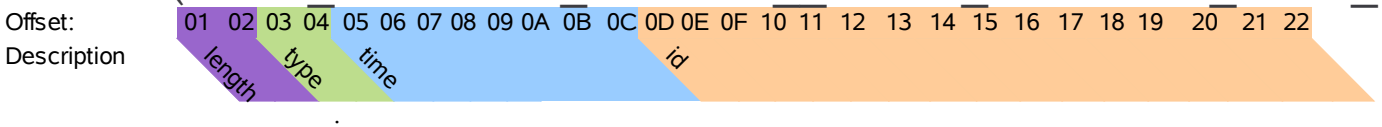


Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0016 VIGIL_ET_MODIFY_zMOD_PRIMARY_NAMESPACE
primaryNameSpaceID	uint32_t	Primary Namespace ID (See table below)

Name Space IDs:

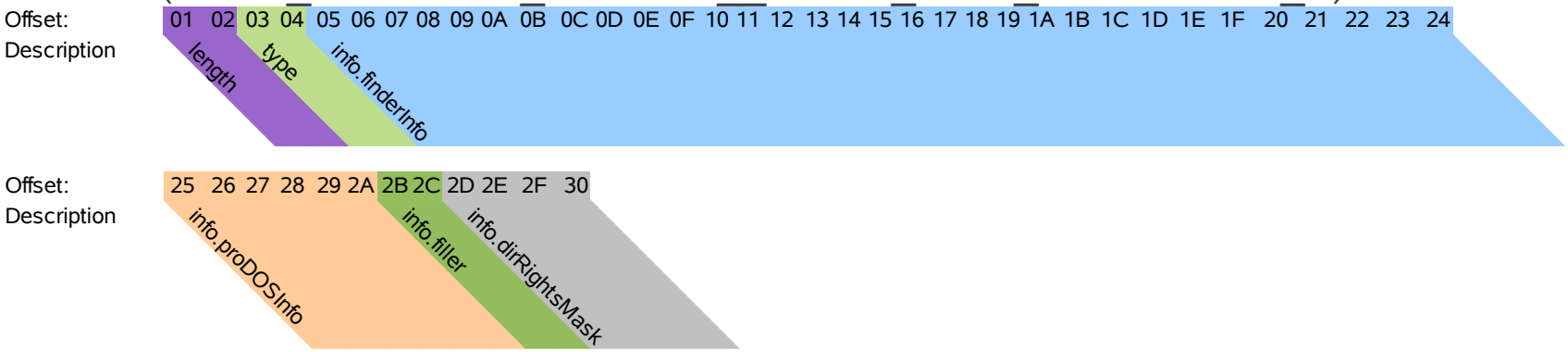
Value	Macro
0	zNSPACE_DOS
1	zNSPACE_MAC
2	zNSPACE_UNIX
3	(DEPRECATED) zNSPACE_FTAM
4	zNSPACE_LONG
5	(UNUSED)
6	zNSPACE_DATA_STREAM
7	zNSPACE_EXTENDED_ATTRIBUTE

0x0017 VIGIL_ET_MODIFY_zMOD_DELETED_INFO (VIGIL_ELEMENT_MODIFY__zMOD_DELETED_INFO_T)



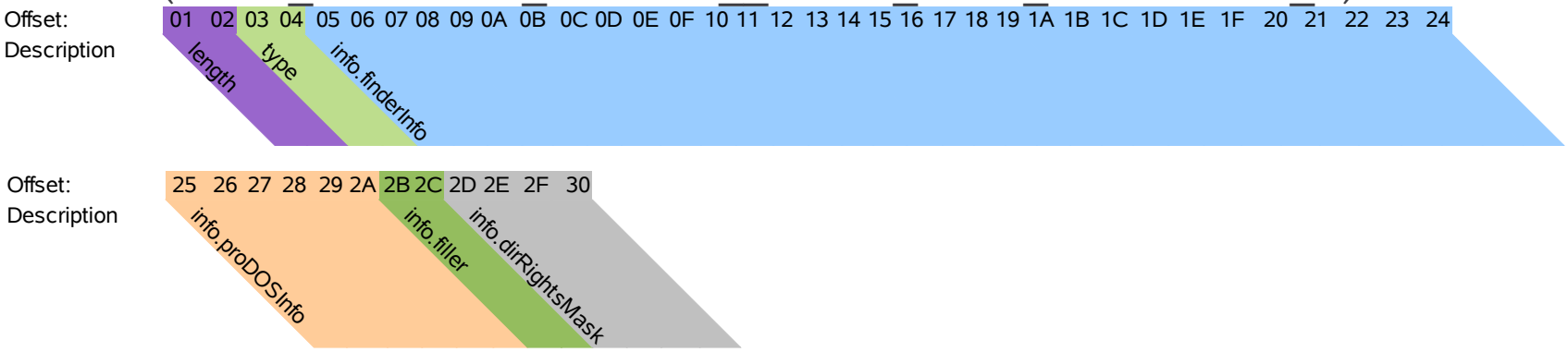
Element:	Type	Description
length	uint16_t	0x0022 Length of element (in bytes).
type	uint16_t	0x0017 VIGIL_ET_MODIFY_zMOD_DELETED_INFO
time	uint64_t	(struct timeval) Delete timestamp.
id	16 Bytes	eDir GUID of object that performed the delete operation

0x0018 VIGIL_ET_MODIFY_zMOD_MAC_METADATA (VIGIL_ELEMENT_MODIFY__zMOD_MAC_METADATA_T)



Element:	Type	Description
length	uint16_t	0x0030 Length of element (in bytes).
type	uint16_t	0x0018 VIGIL_ET_MODIFY_zMOD_MAC_METADATA
info.finderInfo	32 Bytes	
info.proDOSInfo	8 Bytes	
info.filler	2 Bytes	
info.dirRightsMask	uint32_t	

0x0019 VIGIL_ET_MODIFY_zMOD_UNIX_METADATA (VIGIL_ELEMENT_MODIFY__zMOD_UNIX_METADATA_T)

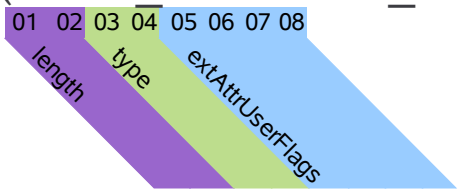


Element:	Type	Description
length	uint16_t	0x0030 Length of element (in bytes).
type	uint16_t	0x0019 VIGIL_ET_MODIFY_zMOD_UNIX_METADATA
info.fMode	uint32_t	
info.rDev	uint32_t	
info.myFlags	uint32_t	
info.nfsUID	uint32_t	
info.nfsGID	uint32_t	
info.nwUID	uint32_t	
info.nwGID	uint32_t	
info.nwEveryone	uint32_t	
info.nwUIDRights	uint32_t	
info.nwGIDRights	uint32_t	
info.nwEveryoneRights	uint32_t	
info.ascFlags	uint8_t	
info.firstCreated	uint8_t	
info.variableSize	uint16_t	If non-zero, there will be variableSize number of additional bytes of metadata in info.variableData.
info.variableData	uint8_t	

0x001A VIGIL_ET_MODIFY_zMOD_EXTATTR_FLAGS (VIGIL_ELEMENT_MODIFY__zMOD_EXTATTR_FLAGS_T)

Offset: 01 02 03 04 05 06 07 08

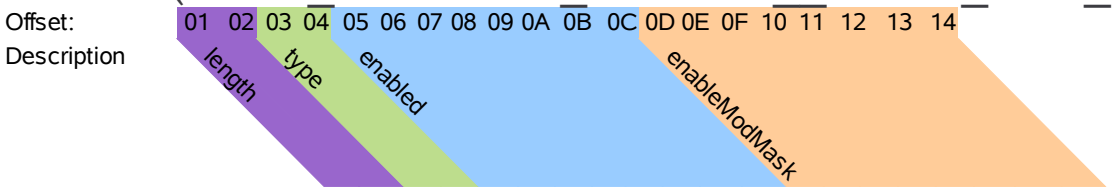
Description



.

Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x001A VIGIL_ET_MODIFY_zMOD_EXTATTR_FLAGS
extAttrUserFlags	uint32_t	Unimplemented/Reserved

0x001B VIGIL_ET_MODIFY_zMOD_VOL_ATTRIBUTES (VIGIL_ELEMENT_MODIFY__zMOD_VOL_ATTRIBUTES_T)

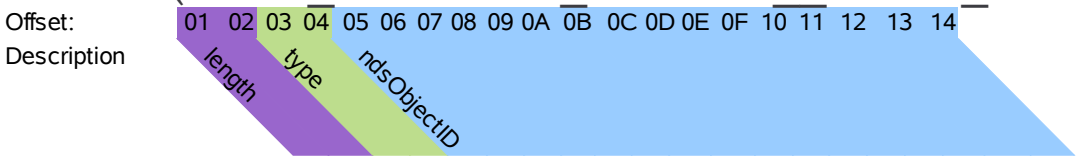


Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x001B VIGIL_ET_MODIFY_zMOD_VOL_ATTRIBUTES
enabled	uint64_t	(See table below)
enableModMask	uint64_t	Bits detailing which volume attributes were modified by this audited event.

Volume Attribute Bits:

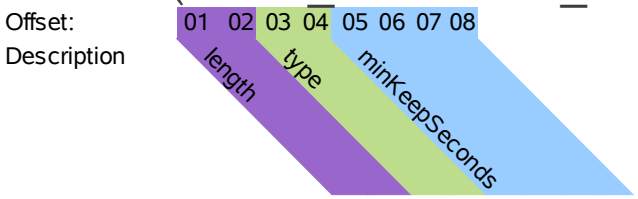
Bit Value	Macro	Bit Value	Macro
0x00000001	zATTR_SALVAGE	0x00010000	zATTR_VERIFY
0x00000002	zATTR_USER_SPACE_RESTRICTIONS	0x00020000	zATTR_REBUILD
0x00000004	zATTR_READONLY	0x00040000	zATTR_COW
0x00000008	zATTR_COMPRESSION	0x00080000	zATTR_VIRTUAL_FILES
0x00000010	zATTR_EXTENDED_ATTRIBUTES	0x00100000	zATTR_USER_TRANSACTION
0x00000020	zATTR_DATA_STREAMS	0x00200000	zATTR_USER_TRANSACTION_ACTIVE
0x00000040	zATTR_DOS_METADATA	0x00400000	zATTR_DONT_BACKUP
0x00000080	zATTR_NETWARE_METADATA	0x00800000	zATTR_MFL
0x00000100	zATTR_MAC_METADATA	0x01000000	zATTR_DIR_QUOTAS
0x00000200	zATTR_UNIX_METADATA	0x02000000	zATTR_SHRED_DATA
0x00000400	zATTR_HARD_LINKS	0x04000000	zATTR_SHARED
0x00000800	zATTR_TRANSACTION	0x08000000	zATTR_HIGH_INTEGRITY
0x00001000	zATTR_SPARSE_FILES	0x10000000	zATTR_MIGRATION
0x00002000	zATTR_PHYSICAL_EOF	0x20000000	zATTR_CFS_MASTER
0x00004000	zATTR_DIRECT_IO	0x40000000	zATTR_CFS_SLAVE
0x00008000	zATTR_PERSISTENT_ATTRIBUTES	0x80000000	zATTR_ENCRYPTED

0x001C VIGIL_ET_MODIFY_zMOD_VOL_NDS_OBJECT_ID (VIGIL_ELEMENT_MODIFY__zMOD_VOL_NDS_OBJECT_ID_T)



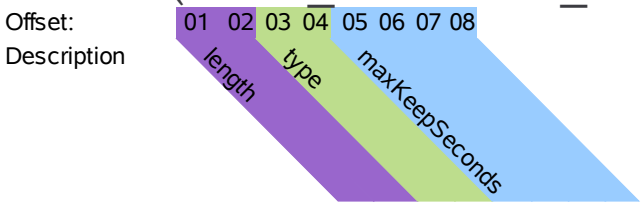
Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x001C VIGIL_ET_MODIFY_zMOD_VOL_NDS_OBJECT_ID
ndsObjectID	16 Bytes	eDir Object GUID

0x001D VIGIL_ET_MODIFY_zMOD_VOL_MIN_KEEP_SECONDS (VIGIL_ELEMENT_MODIFY__zMOD_VOL_MIN_KEEP_SECONDS_T)



Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x001D VIGIL_ET_MODIFY_zMOD_VOL_MIN_KEEP_SECONDS
minKeepSeconds	uint32_t	Minimum seconds a file is kept in the salvage system (after deletion).

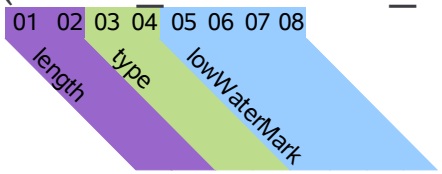
0x001E VIGIL_ET_MODIFY_zMOD_VOL_MAX_KEEP_SECONDS (VIGIL_ELEMENT_MODIFY__zMOD_VOL_MAX_KEEP_SECONDS_T)



Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x001E VIGIL_ET_MODIFY_zMOD_VOL_MAX_KEEP_SECONDS
maxKeepSeconds	uint32_t	Maximum seconds to keep the file in the salvage system when it is deleted.

0x001F VIGIL_ET_MODIFY_zMOD_VOL_LOW_WATER_MARK (VIGIL_ELEMENT_MODIFY__zMOD_VOL_LOW_WATER_MARK_T)

Offset:
Description

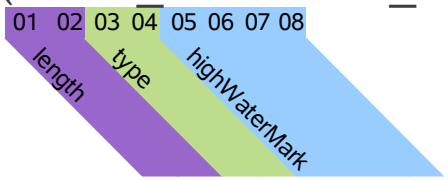


Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x001F VIGIL_ET_MODIFY_zMOD_VOL_LOW_WATER_MARK
lowWaterMark	uint32_t	If the amount of free space drops below this percentage, the file system begins purging deleted files.

0x0020 VIGIL_ET_MODIFY_zMOD_VOL_HIGH_WATER_MARK (VIGIL_ELEMENT_MODIFY__zMOD_VOL_HIGH_WATER_MARK_T)

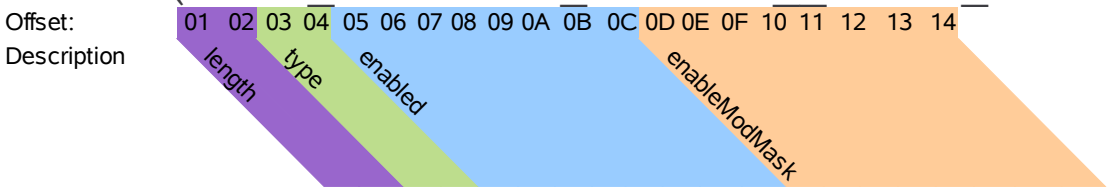
Offset: 01 02 03 04 05 06 07 08

Description



Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0020 VIGIL_ET_MODIFY_zMOD_VOL_HIGH_WATER_MARK
highWaterMark	uint32_t	If there are files to delete, the autopurging process stops when the amount of free space reaches this percentage.

0x0021 VIGIL_ET_MODIFY_zMOD_POOL_ATTRIBUTES (VIGIL_ELEMENT_MODIFY__zMOD_POOL_ATTRIBUTES_T)



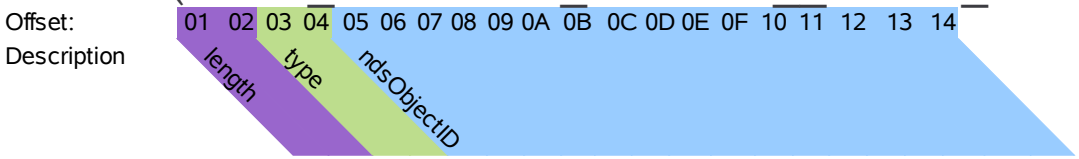
Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0021 VIGIL_ET_MODIFY_zMOD_POOL_ATTRIBUTES
enabled	uint64_t	(See table below)
enableModeMask	uint64_t	Bits detailing which pool attributes were modified by this audited event.

Pool Attribute Bits:

Bit Value	Macro	Meaning
0x00000001	zPOOL_FEATURE_PERSISTENT_FEATURES	Pools features are stored persistently.
0x00000002	zPOOL_FEATURE_SHARED_CLUSTER	Pool is part of a cluster. Potentially accessed by multiple servers.
0x00000004	zPOOL_FEATURE_READ_ONLY	Pool is read only. (No writes can be attempted on the pool).
0x00000008	zPOOL_FEATURE_VERIFY	Pool supports verify after write operation.
0x00000010	zPOOL_FEATURE_REBUILD	Pool supports a rebuild operation.
0x00000020	zPOOL_FEATURE_MULTIPLE_VOLUMES	Pool can support more than 1-to-1 pool-volume relationship.
0x00000040	zPOOL_FEATURE_SNAPSHOT	Indicates that the pool is a snapshot of another pool.
0x00000080	zPOOL_FEATURE_MSAP	MSAP logic should be executed to prevent multiple servers from accessing the pool at the same time.

(All other bit values are reserved and currently undefined.)

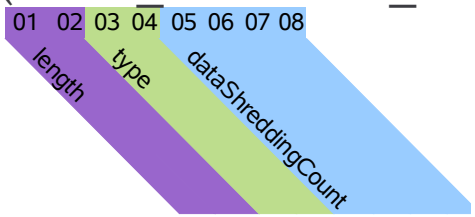
0x0022 VIGIL_ET_MODIFY_zMOD_POOL_NDS_OBJECT_ID (VIGIL_ELEMENT_MODIFY__zMOD_POOL_NDS_OBJECT_ID_T)



Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0022 VIGIL_ET_MODIFY_zMOD_POOL_NDS_OBJECT_ID
ndsObjectID	16 Bytes	eDir Object GUID

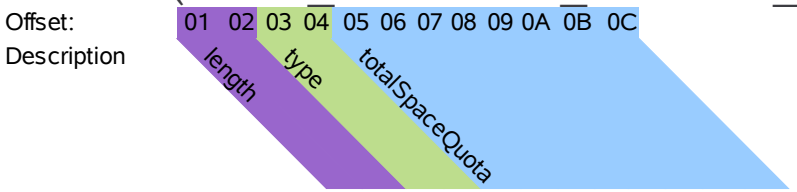
0x0023 VIGIL_ET_MODIFY_zMOD_VOL_DATA_SHREDDING_COUNT (VIGIL_ELEMENT_MODIFY__zMOD_VOL_DATA_SHREDDING_COUNT_T)

Offset:
Description



Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0023 VIGIL_ET_MODIFY_zMOD_VOL_DATA_SHREDDING_COUNT
dataShreddingCount	uint32_t	How many writes are done to obscure the original data. (Up to 7 passes can be specfied).

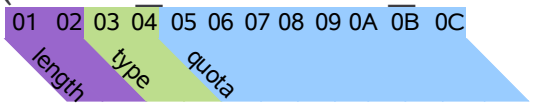
0x0024 VIGIL_ET_MODIFY_zMOD_VOL_QUOTA (VIGIL_ELEMENT_MODIFY__zMOD_VOL_QUOTA_T)



Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x0024 VIGIL_ET_MODIFY_zMOD_VOL_QUOTA
totalSpaceQuota	uint64_t	Maximum size of this volume (may over-book pool).

0x0025 VIGIL_ET_MODIFY_zMOD_DIR_QUOTA (VIGIL_ELEMENT_MODIFY__zMOD_DIR_QUOTA_T)

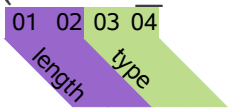
Offset: 01 02 03 04 05 06 07 08 09 0A 0B 0C
Description



Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x0025 VIGIL_ET_MODIFY_zMOD_DIR_QUOTA
quota	uint64_t	Quota size

0x0026 VIGIL_ET_MODIFY_zMOD_READ_AHEAD_BLOCKS (VIGIL_ELEMENT_MODIFY__zMOD_READ_AHEAD_BLOCKS_T)

Offset:
Description

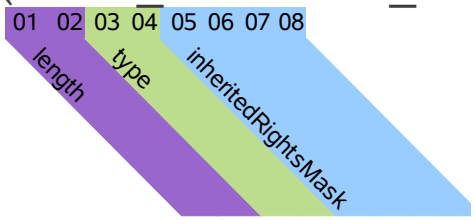


Element:	Type	Description
length	uint16_t	0x0004 Length of element (in bytes).
type	uint16_t	0x0026 VIGIL_ET_MODIFY_zMOD_READ_AHEAD_BLOCKS

0x0027 VIGIL_ET_MODIFY_zMOD_INH_RIGHTS_MASK (VIGIL_ELEMENT_MODIFY__zMOD_INH_RIGHTS_MASK_T)

Offset: 01 02 03 04 05 06 07 08

Description

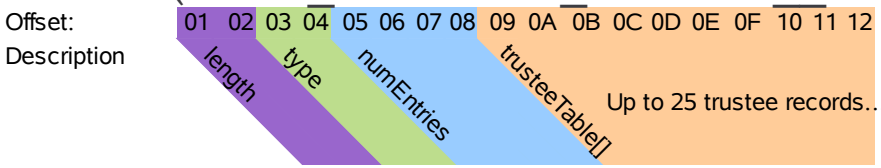


Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0027 VIGIL_ET_MODIFY_zMOD_INH_RIGHTS_MASK
inheritedRightsMask	uint32_t	(See table below)

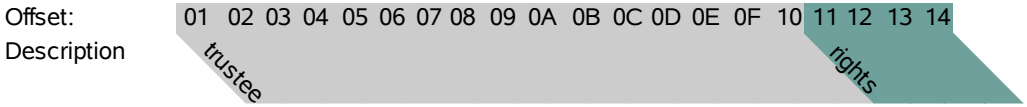
Inherited Rights Mask Bits:

Value	Macro
0x0001	zAUTHORIZE_READ_CONTENTS
0x0002	zAUTHORIZE_WRITE_CONTENTS
0x0008	zAUTHORIZE_CREATE_ENTRY
0x0010	zAUTHORIZE_DELETE_ENTRY
0x0020	zAUTHORIZE_ACCESS_CONTROL
0x0040	zAUTHORIZE_SEE_FILES
0x0080	zAUTHORIZE_MODIFY_METADATA
0x0100	zAUTHORIZE_SUPERVISOR
0x0200	zAUTHORIZE_SALVAGE
0x8000	zAUTHORIZE_SECURE

0x0028 VIGIL_ET_MODIFY_zMOD_ALL_TRUSTEES (VIGIL_ELEMENT_MODIFY__zMOD_ALL_TRUSTEES_T)



Element:	Type	Description
length	uint16_t	Length of element (in bytes).
type	uint16_t	0x0028 VIGIL_ET_MODIFY_zMOD_ALL_TRUSTEES
numEntries	uint32_t	Number of trustee records contained in this record.
trusteeTable	See below	Up to 25 of the below defined structures.

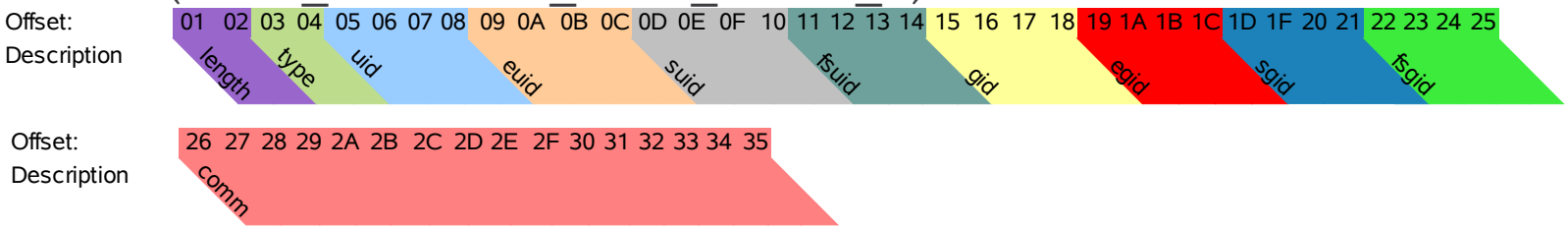


Element:	Type	Description
trustee	16-Bytes	eDir GUID of trustee
rights	uint32_t	(See table below)

Trustee Rights Bits:

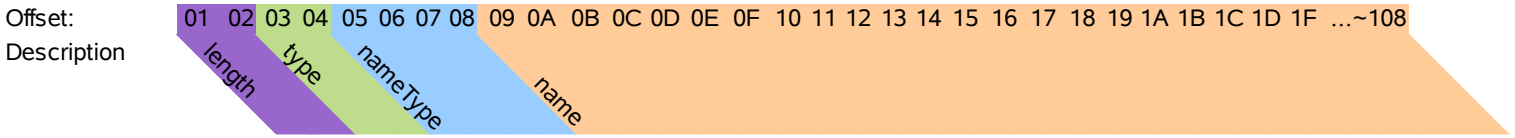
Value	Macro
0x0001	zAUTHORIZE_READ_CONTENTS
0x0002	zAUTHORIZE_WRITE_CONTENTS
0x0008	zAUTHORIZE_CREATE_ENTRY
0x0010	zAUTHORIZE_DELETE_ENTRY
0x0020	zAUTHORIZE_ACCESS_CONTROL
0x0040	zAUTHORIZE_SEE_FILES
0x0080	zAUTHORIZE_MODIFY_METADATA
0x0100	zAUTHORIZE_SUPERVISOR
0x0200	zAUTHORIZE_SALVAGE
0x8000	zAUTHORIZE_SECURE

0x0030 VIGIL_ET_WHO__LINUX
(VIGIL_ELEMENT_WHO_LINUX_T)



Element:	**Type**	**Description**
length	uint16_t	0x0035 Length of element (in bytes).
type	uint16_t	0x0030 VIGIL_ET_WHO_LINUX
uid	uint32_t	“user identifier” of the Linux process which generated this audited event
euid	uint32_t	“Effective user identifier” of the Linux process which generated this audited event.
suid	uint32_t	“Set user identifier” of the Linux process which generated this audited event.
fsuid	uint32_t	“File system user identifier” of the Linux process which generated this audited event.
gid	uint32_t	“group identifier” of the Linux process which generated this audited event.
egid	uint32_t	“Effective group identifier” of the Linux process which generated this audited event.
sgid	uint32_t	“Set group identifier” of the Linux process which generated this audited event.
fsgid	uint32_t	“File system group identifier” of the Linux process which generated this audited event.
comm	16 Bytes	(string)Name of Linux user-space application which generated this audited event.

0x0034 VIGIL_ET_NAME (VIGIL_ELEMENT_NAME_T)

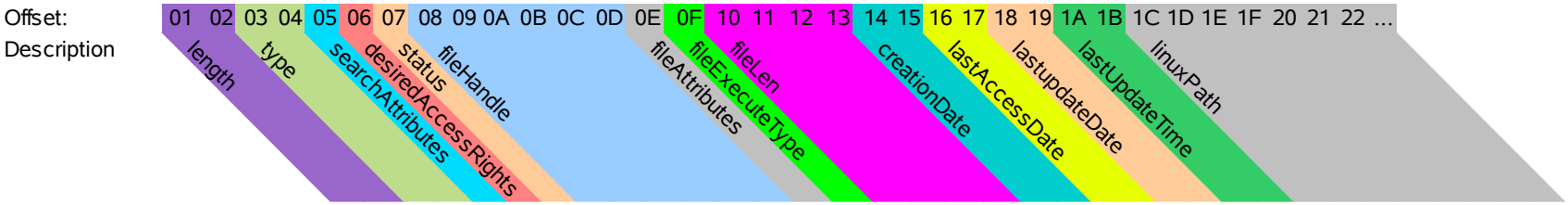


Element:	Type	Description
length	uint16_t	Length of element (in bytes).
type	uint16_t	0x0034 VIGIL_ET_NAME_LINUX
nameType	uint32_t	(See table below)
name	string	Name string.

Name types:

Value	Macro	Description
0x00000000	VIGIL_ELEMENT_NAMETYPE_NONE	Non-described type
0x00000001	VIGIL_ELEMENT_NAMETYPE_CLIENT	Vigil auditing client name.
0x00000002	VIGIL_ELEMENT_NAMETYPE_CLIENTUSER	Vigil auditing client user name.

0x0035 VIGIL_ET_NCP_LOCAL_OPENFILE (VIGIL_ELEMENT_NCP_OPENFILE_T)



Element:	Type	Description
length	uint16_t	Length of element (in bytes).
type	uint16_t	0x0035 VIGIL_ET_NCP_LOCAL_OPENFILE
searchAttributes	uint8_t	(See "Search Attributes" table below)
desiredAccessRights	uint8_t	(See "Desired Access Rights" table below)
status	uint8_t	0=Audited operation success. Non-zero=Audited operation error code.
fileHandle	6 Bytes	NCP engine assigned file handle.
fileAttributes	uint8_t	(See "File Attributes" table.)
fileExecuteType	uint8_t	(unimplemented. Always zero)
fileLen	uint32_t	File size in bytes.
creationDate	uint16_t	(See "Date Format" table below.)
lastAccessedDate	uint16_t	(See "Date Format" table below.)
lastUpdateDate	uint16_t	(See "Date Format" table below.)
lastUpdateTime	uint16_t	(See "Time Format" table below.)
linuxPath	string	File path as it would be referenced in the Linux filesystem

File Attributes:

Bit	Meaning
0x01	Read only
0x02	Hidden
0x04	System
0x08	Execute
0x10	Subdirectory
0x20	Archive
0x80	Shareable

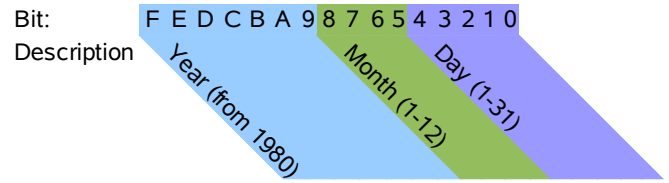
Search Attributes:

Bit	Meaning
0x01	Hidden
0x02	System
0x04	Sudirectories Only
0x0F	All Files and Subdiectories

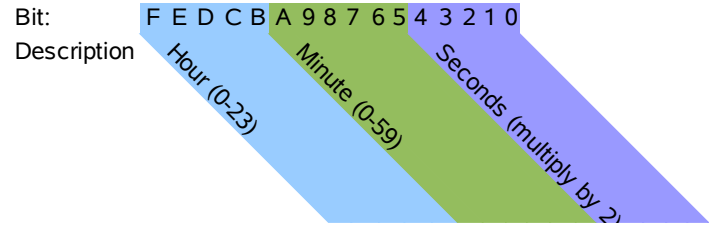
Desired Access Rights:

Value	Mode
0	Read only
1	Write only
2	Deny read
3	Deny write
4	Compatibility
6	File write through
10	Delete file close

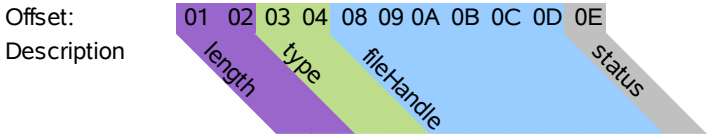
Date Format:



Time Format:

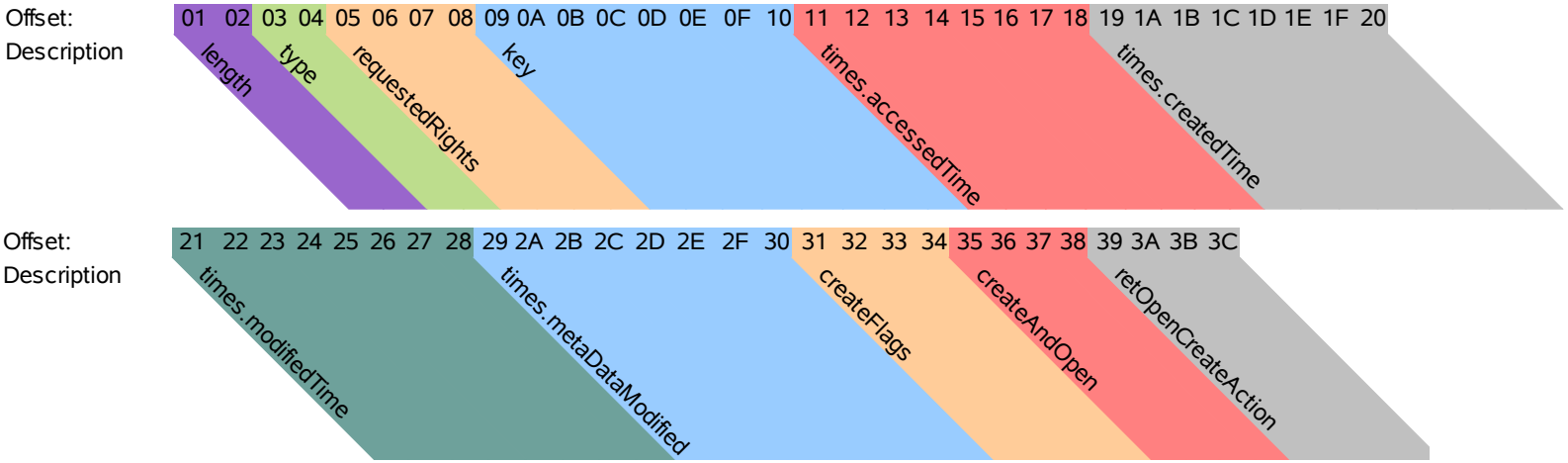


0x0036 VIGIL_ET_NCP_LOCAL_CLOSEFILE (VIGIL_ELEMENT_NCP_CLOSEFILE_T)



Element:	Type	Description
length	uint16_t	0x000E Length of element (in bytes).
type	uint16_t	0x0036 VIGIL_ET_NCP_LOCAL_CLOSEFILE
fileHandle	6 Bytes	NCP engine assigned file handle.
status	uint8_t	0=Audited operation success. Non-zero=Audited operation error code.

0x0038 VIGIL_ET_NSS_CREATE (VIGIL_ELEMENT_NSS_Create_T)



Element:	Type	Description
length	uint16_t	0x003C Length of element (in bytes).
type	uint16_t	0x0038 VIGIL_ET_NSS_CREATE
requestedRights	uint32_t	(See “Requested Rights” table on next page)
key	int64_t	NSS file handle.
times.accessedTime	uint64_t	(struct timeval) timestamp of last file access.
times.createdTime	uint64_t	(struct timeval) file creation timestamp.
times.modifiedTime	uint64_t	(struct timeval) timestamp of last file content modification.
times.metaDataModifiedTime	uint64_t	(struct timeval) timestamp of last file metadata modification.
createFlags	uint32_t	(See “Create Flags” table below)
createAndOpen	uint32_t	0[FALSE]=Create only. !0[TRUE]=Create and open.
retOpenCreateAction	uint32_t	(See “Open/Create Action” table below)

Create Flags:

Bit	Macro	Notes
0x00000001	zCREATE_OPEN_IF_THERE	
0x00000002	zCREATE_TRUNCATE_IF_THERE	
0x00000004	zCREATE_DELETE_IF_THERE	
0x00000100	zCREATE_KEEP_VFS_CACHE	Internal NSS use only.

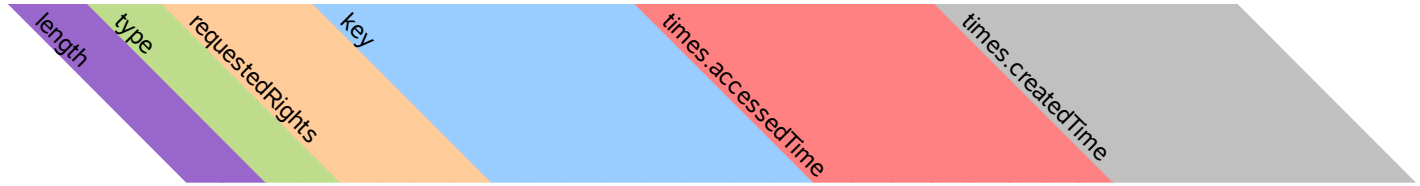
Open/Create Action:

Bit	Macro	Notes
0x00000001	zBEAST_EXISTED	The NSS object previously existed.
0x00000002	zBEAST_CREATED	The NSS object was created/re-created.
0x00000004	zBEAST_TRUNCATED	The NSS object existed and was truncated.

	Bit	Macro	Meaning
Requested Rights:	0x00000001	zRR_READ_ACCESS	Read access to (file) object.
	0x00000002	zRR_WRITE_ACCESS	Write access to (file) object.
	0x00000004	zRR_DENY_READ	Exclusive read. (Nobody else can open for reading).
	0x00000008	zRR_DENY_WRITE	Exculsive write (Nobody else can open for writing).
	0x00000010	zRR_SCAN_ACCESS	Scan access to (file) object
	0x00000020	(Reserved)	
	0x00000040	(Reserved)	
	0x00000080	(Reserved)	
	0x00000100	zRR_ENABLE_IO_ON_COMPRESSSED_DATA	
	0x00000200	zRR_LEAVE_FILE_COMPRESSED	
	0x00000400	zRR_DELETE_FILE_ON_CLOSE	Delete the file when it is closed.
	0x00000800	zRR_FLUSH_ON_CLOSE	Flush all (file) data blocks when it is closed.
	0x00001000	zRR_PURGE_IMMEDIATE_ON_CLOSE	If (file) is deleted on close, do not allow the file to be salvaged.
	0x00002000	zRR_DIO_MODE	Open (file) in direct I/O mode (May conflict with other modes).
	0x00004000	(Reserved)	
	0x00008000	(Reserved)	
	0x00010000	(Reserved)	
	0x00020000	zRR_ALLOW_SECURE_DIRECTORY_ACCESS	
	0x00040000	(Reserved)	
	0x00080000	(Reserved)	
	0x00100000	zRR_TRANSACTION_ACTIVE	Have the file use the default transaction.
	0x00200000	zRR_PSA_CACHE	
	0x00400000	(Reserved)	
	0x00800000	(Reserved)	
	0x01000000	zRR_PREVENT_FS_HOOKS	Internal use only bit. If set, FS_HOOKS will not be activated during open/close events.
	0x02000000	zRR_MASK_READ_IN_DROP_BOXES	
	0x04000000	zRR_READ_ACCESS_TO_SNAPSHOT	
	0x08000000	zRR_DENY_RW_OPENER_CAN_REOPEN	
	0x10000000	zRR_CREATE_WITHOUT_READ_ACCESS	Give only write access to the file when created.
	0x20000000	zRR_OPENER_CAN_DELETE_WHILE_OPEN	Only the opener of the file can delete the file while it is open.
	0x40000000	zRR_CANT_DELETE_WHILE_OPEN	Don't let anyone delete this file while it is open.
	0x80000000	zRR_DONT_UPDATE_ACCESS_TIME	Don't update the access time. (Intended for backup, malware scans, etc.

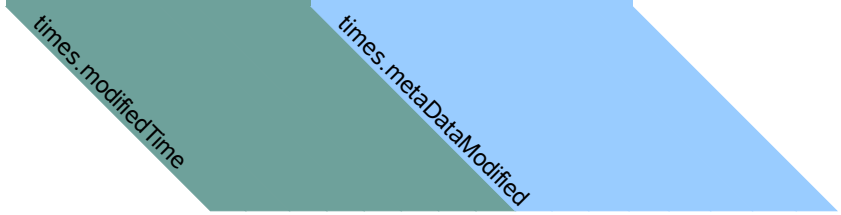
0x0039 VIGIL_ET_NSS_OPEN (VIGIL_ELEMENT_NSS_Open_T)

Description



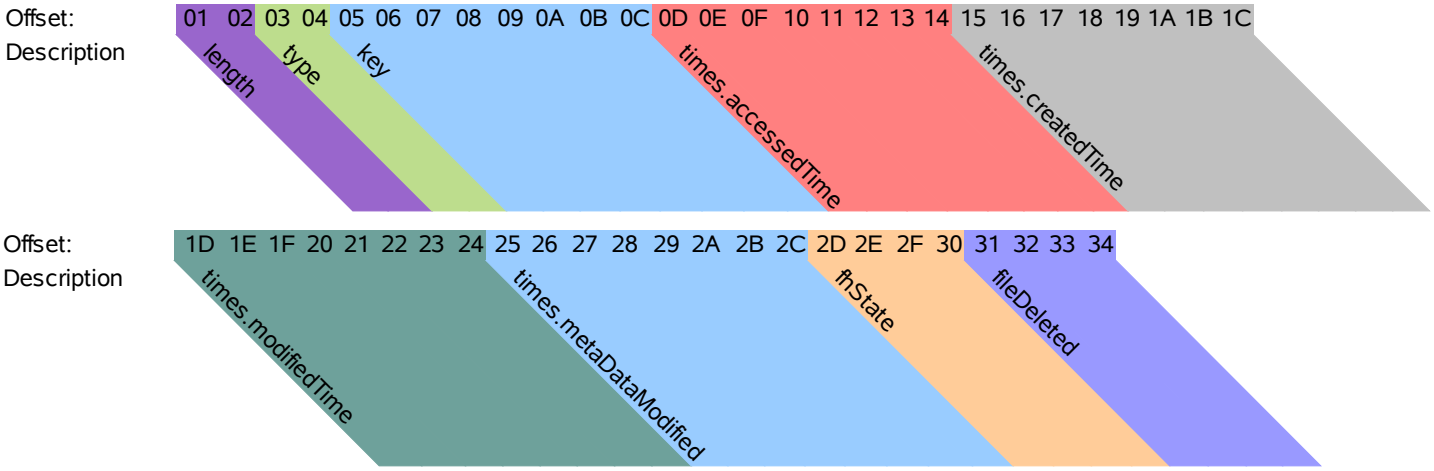
Offset: 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F 30

Description



Element:	Type	Description
length	uint16_t	0x0030 Length of element (in bytes).
type	uint16_t	0x0039 VIGIL_ET_NSS_OPEN
requestedRights	uint32_t	(See “Requested Rights” table on previous page)
key	int64_t	NSS file handle.
times.accessedTime	uint64_t	(struct timeval) timestamp of last file access.
times.createdTime	uint64_t	(struct timeval) file creation timestamp.
times.modifiedTime	uint64_t	(struct timeval) timestamp of last file content modification.
times.metaDataModifiedTime	uint64_t	(struct timeval) timestamp of last file metadata modification.

0x003A VIGIL_ET_NSS_CLOSE (VIGIL_ELEMENT_NSS_Close_T)



Element:	Type	Description
length	uint16_t	0x0034 Length of element (in bytes).
type	uint16_t	0x003A VIGIL_ET_NSS_CLOSE
key	int64_t	NSS file handle.
times.accessedTime	uint64_t	(struct timeval) timestamp of last file access.
times.createdTime	uint64_t	(struct timeval) file creation timestamp.
times.modifiedTime	uint64_t	(struct timeval) timestamp of last file content modification.
times.metaDataModifiedTime	uint64_t	(struct timeval) timestamp of last file metadata modification.
fhState	uint32_t	(See “Filehandle States” table below)
fileDeleted	uint32_t	Non-zero[TRUE] indcates that the file was deleted when closed.

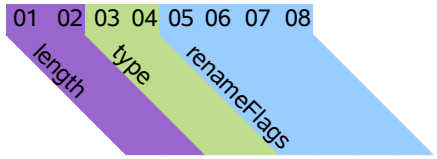
Filehandle States:

Bit	Macro	Notes
0x01	FH_NEW	
0x02	FH_MODIFIED	File content (specific to this file handle instance) was modified while open
0x04	FH_WRITE_SNAPSHOT	
0x08	FH_READ_BACKUP	
0x10	FH_NDS_OPEN	Open performed for CFS slave on the master.
0x20	FH_CFS_ASYNC_CLOSE	Pre-close

0x003B VIGIL_ET_NSS_RENAME (VIGIL_ELEMENT_NSS_Rename_T)

Offset: 01 02 03 04 05 06 07 08

Description

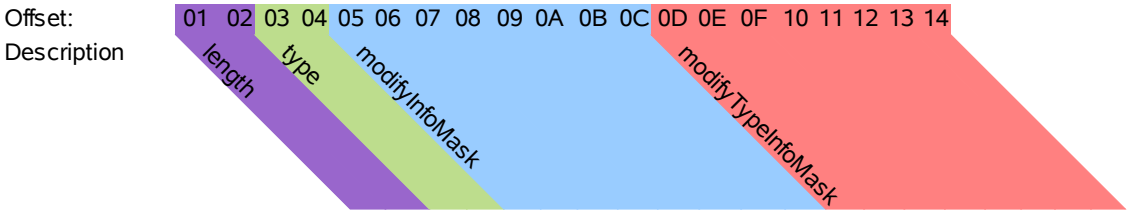


Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x003B VIGIL_ET_NSS_RENAME
renameFlags	uint32_t	(See “Rename Flags” table below).

Rename Flags:

Bit	Macro	Notes
0x00000001	zRENAME_ALLOW_RENAMES_TO_MYSELF	
0x00000002	zRENAME_COMPATABILITY	
0x00000008	zRENAME_THIS_NAME_SPACE_ONLY	
0x00000010	ZRENAME_DON”T_RENAME_FILES	Internal NSS use only.
0x00000020	ZRENAME_DON”T_RENAME_DIRECTORIES	Internal NSS use only.
0x00000040	ZRENAME_TARGET_IS_PATTERN	Internal NSS use only.
0x00000100	ZRENAME_KEEP_VFS_CACHE	Internal NSS use only.

0x003C VIGIL_ET_NSS_MODIFYINFO (VIGIL_ELEMENT_NSS_ModifyInfo_T)

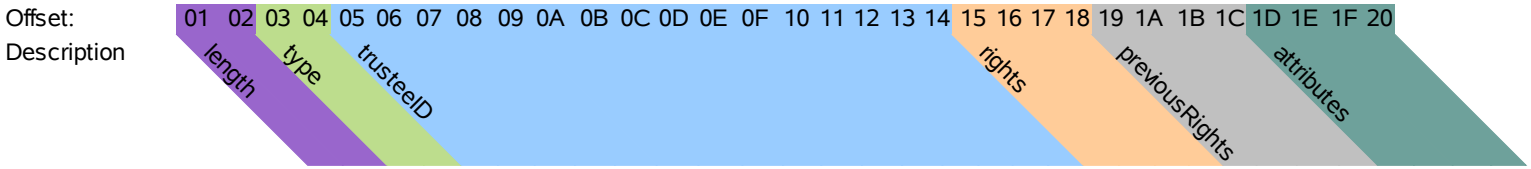


Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x003C VIGIL_ET_NSS_MODIFYINFO
modifyInfoMask	uint64_t	(See “Modify Info Mask” table below).
modifyTypeInfoMask	uint64_t	(Not Implemented. Do not reference.).

ModifyInfo Mask Bits:

Bit	Macro
0x00000001	zMOD_FILE_ATTRIBUTES
0x00000002	zMOD_CREATED_TIME
0x00000004	zMOD_ARCHIVED_TIME
0x00000008	zMOD_MODIFIED_TIME
0x00000010	zMOD_ACCESSED_TIME
0x00000020	zMOD_METADATA_MODIFIED_TIME
0x00000040	zMOD_OWNER_ID
0x00000080	zMOD_ARCHIVER_ID
0x00000100	zMOD_MODIFIER_ID
0x00000200	zMOD_METADATA_MODIFIER_ID
0x00000400	zMOD_PRIMARY_NAMESPACE
0x00000800	zMOD_DELETED_INFO
0x00001000	zMOD_MAC_METADATA
0x00002000	zMOD_UNIX_METADATA
0x00004000	zMOD_EXTATTR_FLAGS
0x00008000	zMOD_VOL_ATTRIBUTES
0x00010000	zMOD_VOL_NDS_OBJECT_ID
0x00020000	zMOD_VOL_MIN_KEEP_SECONDS
0x00040000	zMOD_VOL_MAX_KEEP_SECONDS
0x00080000	zMOD_VOL_LOW_WATER_MARK
0x00100000	zMOD_VOL_HIGH_WATER_MARK
0x00200000	zMOD_POOL_ATTRIBUTES
0x00400000	zMOD_POOL_NDS_OBJECT_ID
0x00800000	zMOD_VOL_DATA_SHREDDING_COUNT
0x01000000	zMOD_VOL_QUOTA
0x02000000	zMOD_DIR_QUOTA
0x04000000	zMOD_READ_AHEAD_BLOCKS
0x08000000	zMOD_INH_RIGHTS_MASK

0x003D VIGIL_ET_NSS_ADDTRUSTEE (VIGIL_ELEMENT_NSS_AddTrustee_T)



Element:	Type	Description
length	uint16_t	0x0020 Length of element (in bytes).
type	uint16_t	0x003D VIGIL_ET_NSS_ADDTRUSTEE
trusteeID	16 Bytes	eDir GUID of trustee targeted for this event.
rights	uint32_t	Rights to add. (See “Trustee Rights” table below).
previousRights	uint32_t	Rights of trustee prior to this event (See “rights” table below).
attributes	uint32_t	(See “Authorization Attributes” table below).

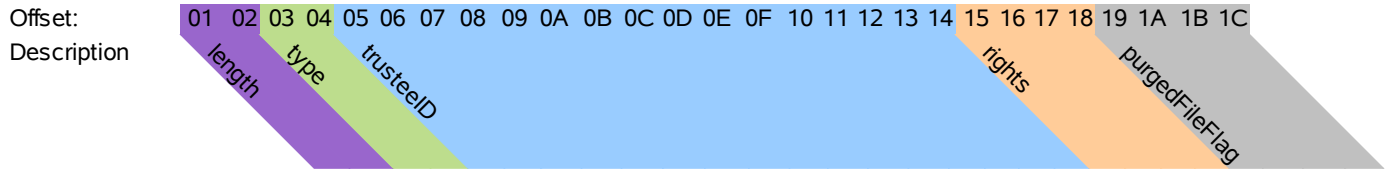
Trustee Rights Bits:

Bit	Macro
0x00000001	zAUTHORIZE_READ_CONTENTS
0x00000002	zAUTHORIZE_WRITE_CONTENTS
0x00000008	zAUTHORIZE_CREATE_ENTRY
0x00000010	zAUTHORIZE_DELETE_ENTRY
0x00000020	zAUTHORIZE_ACCESS_CONTROL
0x00000040	zAUTHORIZE_SEE_FILES
0x00000080	zAUTHORIZE_MODIFY_METADATA
0x00000100	zAUTHORIZE_SUPERVISOR
0x00000200	zAUTHORIZE_SALVAGE
0x00008000	zAUTHORIZE_SECURE

Authorization Attributes Bits:

Bit	Macro
0x00002000	zAUTHORIZE_NEGATIVE_RIGHTS
0x00004000	zAUTHORIZE_INHERIT_UP
0x00008000	zAUTHORIZE_INHERIT_DOWN

0x003E VIGIL_ET_NSS_REMOVETRUSTEE (VIGIL_ELEMENT_NSS_RemoveTrustee_T)



Element:	Type	Description
length	uint16_t	0x001C Length of element (in bytes).
type	uint16_t	0x003E VIGIL_ET_NSS_REMOVETRUSTEE
trusteeID	16 Bytes	eDir GUID of trustee targeted for this event.
rights	uint32_t	Rights to remove. (See “Trustee Rights” table below).
puredFileFlag	uint32_t	Non-zero[TRUE] indicates that operation is due to deletion of NSS target object (ie:file).

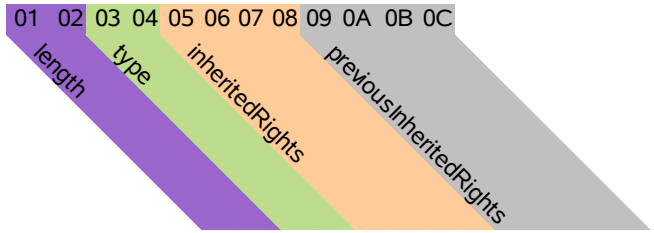
Trustee Rights Bits:

Bit	Macro
0x00000001	zAUTHORIZE_READ_CONTENTS
0x00000002	zAUTHORIZE_WRITE_CONTENTS
0x00000008	zAUTHORIZE_CREATE_ENTRY
0x00000010	zAUTHORIZE_DELETE_ENTRY
0x00000020	zAUTHORIZE_ACCESS_CONTROL
0x00000040	zAUTHORIZE_SEE_FILES
0x00000080	zAUTHORIZE_MODIFY_METADATA
0x00000100	zAUTHORIZE_SUPERVISOR
0x00000200	zAUTHORIZE_SALVAGE
0x00008000	zAUTHORIZE_SECURE

0x003F VIGIL_ET_NSS_SETINHERITEDRIGHTS (VIGIL_ELEMENT_NSS_SetInheritedRights_T)

Offset: 01 02 03 04 05 06 07 08 09 0A 0B 0C

Description

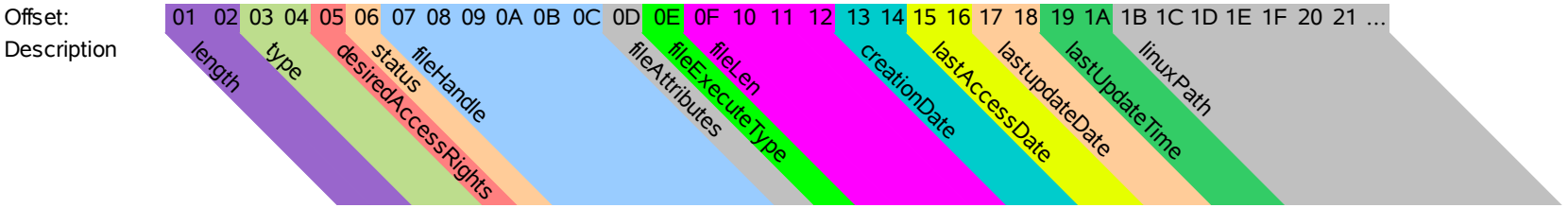


Element:	Type	Description
length	uint16_t	0x000C Length of element (in bytes).
type	uint16_t	0x003F VIGIL_ET_NSS_SETINHERITEDRIGHTS
inheritedRights	uint32_t	Inherited rights being set by this audited event. (See “Inherited Rights” table below).
prevousInheritedRights	uint32_t	Inherited rights, as they existed prior to this event (See “Inherited Rights” table below).

Inherited Rights Bits:

Bit	Macro
0x00000001	zAUTHORIZE_READ_CONTENTS
0x00000002	zAUTHORIZE_WRITE_CONTENTS
0x00000008	zAUTHORIZE_CREATE_ENTRY
0x00000010	zAUTHORIZE_DELETE_ENTRY
0x00000020	zAUTHORIZE_ACCESS_CONTROL
0x00000040	zAUTHORIZE_SEE_FILES
0x00000080	zAUTHORIZE_MODIFY_METADATA
0x00000100	zAUTHORIZE_SUPERVISOR
0x00000200	zAUTHORIZE_SALVAGE
0x00008000	zAUTHORIZE_SECURE

0x0040 VIGIL_ET_CIFS_LOCAL__OPENFILE (VIGIL_ELEMENT_CIFS_OPENFILE_T)



Element:	Type	Description
length	uint16_t	Length of element (in bytes).
type	uint16_t	0x0040 VIGIL_ET_CIFS_LOCAL__OPENFILE
desiredAccessRights	uint8_t	(See "Desired Access Rights" table below)
status	uint8_t	0=Audited operation success. Non-zero=Audited operation error code.
fileHandle	6 Bytes	CIFS engine assigned file handle.
fileAttributes	uint8_t	(See "File Attributes" table.)
fileExecuteType	uint8_t	(unimplemented. Always zero)
fileLen	uint32_t	File size in bytes.
creationDate	uint16_t	(See "Date Format" table below.)
lastAccessedDate	uint16_t	(See "Date Format" table below.)
lastUpdateDate	uint16_t	(See "Date Format" table below.)
lastUpdateTime	uint16_t	(See "Time Format" table below.)
linuxPath	string	File path as it would be referenced in the Linux filesystem

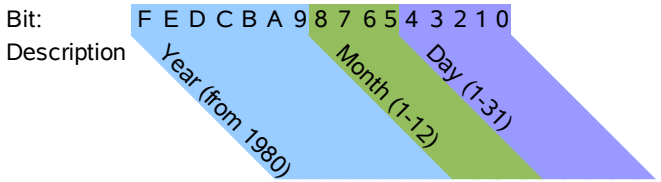
File Attributes:

Bit	Meaning
0x01	Read only
0x02	Hidden
0x04	System
0x08	Execute
0x10	Subdirectory
0x20	Archive
0x80	Shareable

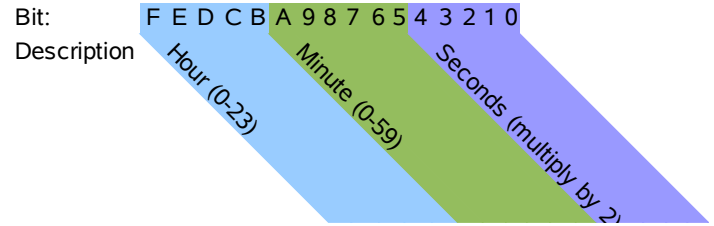
Desired Access Rights:

Value	Mode
0	Read only
1	Write only
2	Deny read
3	Deny write
4	Compatibility
6	File write through
10	Delete file close

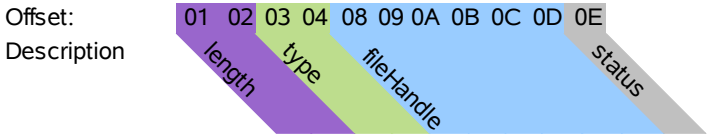
Date Format:



Time Format:

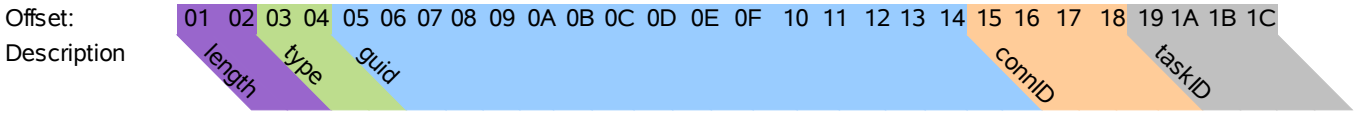


0x0041 VIGIL_ET_CIFS_LOCAL__CLOSEFILE (VIGIL_ELEMENT_CIFS_CLOSEFILE_T)



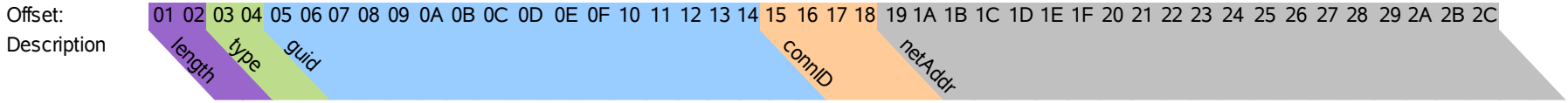
Element:	Type	Description
length	uint16_t	0x000E Length of element (in bytes).
type	uint16_t	0x0041 VIGIL_ET_CIFS_LOCAL)_CLOSEFILE
fileHandle	6 Bytes	CIFS engine assigned file handle.
status	uint8_t	0=Audited operation success. Non-zero=Audited operation error code.

0x0042 VIGIL_ET_PMD_NCP (VIGIL_ELEMENT_PMD_NCP_T)



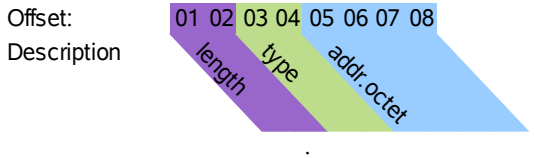
Element:	Type	Description
length	uint16_t	0x001C Length of element (in bytes).
type	uint16_t	0x0042 VIGIL_ET_PMD_NCP
guid	16 Bytes	eDir GUID of the NCP client who initiated the request which resulted in this audited event.
connID	uint32_t	NCP engine connection ID
taskID	uint32_t	NCP client assigned taskID

0x0043 VIGIL_ET_PMD_CIFS (VIGIL_ELEMENT_PMD_CIFS_T)



Element:	Type	Description
length	uint16_t	0x001C or 0x002C Length of element (in bytes).
type	uint16_t	0x0043 VIGIL_ET_PMD_CIFS
guid	16 Bytes	eDir GUID of the CIFS client who initiated the request which resulted in this audited event.
connID	uint32_t	CIFS engine (assigned) connection ID
netAddr	8 or 20 bytes	Encapsulated type 0x0044 or 0x0045 element. (See those element for specific structure definitions).

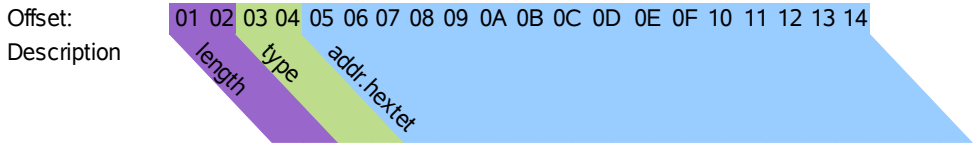
0x0044 VIGIL_ET_NET_ADDR_IPv4 (VIGIL_ELEMENT_NET_ADDR_T)



.

Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0044 VIGIL_ET_NET_ADDR_IPv4
addr.octet	4 bytes	IPv4 address value

0x0045 VIGIL_ET_NET_ADDR_IPv6 (VIGIL_ELEMENT_NET_ADDR_T)

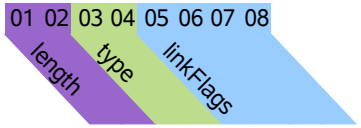


.

Element:	Type	Description
length	uint16_t	0x0014 Length of element (in bytes).
type	uint16_t	0x0045 VIGIL_ET_NET_ADDR_IPv6
addr.hextet	16 Bytes	IPv6 address value

0x0046 VIGIL_ET_NSS_LINK (VIGIL_ELEMENT_NSS_Link_T)

Offset:
Description



.

Element:	Type	Description
length	uint16_t	0x0008 Length of element (in bytes).
type	uint16_t	0x0046 VIGIL_ET_NSS_LINK
linkFlags	uint32_t	(See “Link Flags” table below).

Link Flags:

Bit	Macro	Notes
0x00000001	zLF_HARD_LINK	
0x00000100	zLF_KEEP_VFS_CACHE	NSS internal use only.