NAME

audit_class – audit class definitions

SYNOPSIS

/etc/security/audit_class

AVAILABILITY

The functionality described in this man page is available only if the Basic Security Module (BSM) has been enabled. See **bsmconv**(1M) for more information.

DESCRIPTION

/etc/security/audit_class is an ASCII system file that stores class definitions. Programs use the **getauclassent**(3) routines to access this information.

The fields for each class entry are separated by colons. Each class entry is a bitmap and is separated from each other by a newline.

Each entry in the audit_class file has the form:

mask:*name*:*description*

The fields are defined as follows:

mask	The class mask.
name	The class name.
description	The description of the class.

The classes are now user-configurable. Each class is represented as a bit in the class mask which is an unsigned integer. Thus, there are 32 different classes available, plus two meta-classes -- **all** and **no**.

all represents a conjunction of all allowed classes, and is provided as a shorthand method of specifying all classes.

no is the "invalid" class, and any event mapped solely to this class will not be audited. (Turning auditing on to the **all** meta class will NOT cause events mapped solely to the **no** class to be written to the audit trail.)

EXAMPLES

Here is a sample of a **audit_class** file:

```
0x00000000:no:invalid class
0x00000001:fr:file read
0x00000002:fw:file write
0x00000004:fa:file attribute access
0x00000008:fm:file attribute modify
0x00000010:fc:file create
0x00000020:fd:file delete
0x00000040:cl:file close
0xffffffff:all:all classes
```

FILES

/etc/security/audit_class

SEE ALSO

bsmconv(1M), **getauclassent**(3), **audit_event**(4)

NOTES

It is possible to deliberately turn on the **no** class in the kernel, in which case the audit trail will be flooded with records for the audit event AUE_NULL.