

NAME

aide.conf - The configuration file for Advanced Intrusion Detection Environment

SYNOPSIS

aide.conf is the configuration file for Advanced Intrusion Detection Environment. **aide.conf** contains the runtime configuration aide uses to initialize or check the aide database.

FILE FORMAT

aide.conf is similar in to Tripwire(tm)'s configuration file. With little effort tw.conf can be converted to aide.conf.

Aide.conf is case-sensitive. Leading and trailing whitespaces are ignored.

There are three types of lines in **aide.conf**. First there are the configuration lines which are used to set configuration parameters and define/undefine variables. Second, there are lines that used to select which files are added to the database. Third there are the macrolines. Only the second type of lines are required for aide to do anything. Lines beginning with # are ignored as comments.

CONFIG LINES

These lines have the format parameter=value. See URLs for a list of valid urls.

database

The url from which database is read. There can only be one of these lines. If there are multiple database lines then the first is used. The default value is `"/aide.db"`.

database_out

The url to which the new database is written to. There can only be one of these lines. If there are multiple database_out lines then the first is used. The default value is `"/aide.db.new"`.

database_new

The url from which the other database for --compare is read. There is no default for this one.

verbose The level of messages that is output. This value can be 0-255 inclusive. This parameter can only be given once. Value from the first occurrence is used. If --verbose or -V is used then the value from that is used. The default is 5. If verbosity is 20 then additional report output is written when doing --check, --update or --compare.

report_url

The url that the output is written to. There can be multiple instances of this parameter. Output is written to all of them. The default is stdout.

gzip_dbout

Whether the output to the database is gzipped or not. Valid values are yes,true,no and false. The default is no. This option is available only if zlib support is compiled in.

acl_no_symlink_follow

Whether to check ACLs for symlinks or not. Valid values are yes,true,no and false. The default is to follow symlinks. This option is available only if acl support is compiled in.

warn_dead_symlinks

Whether to warn about dead symlinks or not. Valid values are yes,true,no and false. The default is not to warn about dead symlinks.

ignore_list

Special group definition that lists parameter which are to be ignored from the final report.

config_version

The value of config_version is printed in the report and also printed to the database. This is for informational purposes only. It has no other functionality.

Group definitions

If the parameter is not one of the previous parameters then it is regarded as a group definition. Value is then regarded as an expression. Expression is of the following form.

```
<predefined group>| <expr> + <predefined group>          | <expr> - <predefined group>
```

See DEFAULT GROUPS for an explanation of default predefined groups. Note that this is different from the way Tripwire(tm) does it.

There is also a special group named "ignore_list". The predefined groups listed in it are NOT displayed in the final report.

SELECTION LINES

There are three types of selection lines (regular, negative, equals) Lines beginning with "/" are regular selective lines. Lines beginning with "!" are negative selection lines. And lines beginning with "=" are equals selection lines. The string following the first character is taken as a regular expression matching to a complete filename (with path included). In regular selection rule the "/" is included in the regular expression. Following the regular expression in an expression. See CONFIG LINES for an explanation of expressions. See EXAMPLES and doc/aide.conf for examples.

MACRO LINES

@@define VAR val

Define variable **VAR** to value **val**.

@@undef VAR

Undefine variable **VAR**.

@@ifdef VAR, @@ifndef VAR

@@ifdef begins an if statement. It must be terminated with an **@@endif** statement. The lines between **@@ifdef** and **@@endif** are used if variable **VAR** is defined. If there is an **@@else** statement then the part between **@@ifdef** and **@@else** is used if **VAR** is defined otherwise the part between **@@else** and **@@endif** is used. **@@ifndef** reverses the logic of **@@ifdef** statement but otherwise works similarly.

@@ifhost hostname, @@ifnhost hostname

@@ifhost works like **@@ifdef** only difference is that it checks whether **hostname** equals the name of the host that aide is running on. **hostname** is the name of the host without the domain-name (hostname, not hostname.aide.org).

@{VAR}

@{VAR} is replaced with the value of the variable **VAR**. If variable **VAR** is not defined an empty string is used. Unlike Tripwire(tm) **@@VAR** is NOT supported.

@@else

Begins the else part of an if statement.

@@endif

Ends an if statement.

@@include VAR

Includes the file **VAR**. The content of the file is used as if it were inserted in this part of the config file.

URLS

Urls can be one of the following. Input urls cannot be used as outputs and vice versa.

stdout

stderr Output is sent to stdout,stderr respectively.

stdin Input is read from stdin.

file://filename

Input is read from **filename** or output is written to **filename**.

fd:number

Input is read from filedescriptor **number** or output is written to **number**.

DEFAULT GROUPS

p: permissions
 i: inode
 n: number of links
 u: user
 g: group
 s: size
 m: mtime
 a: atime
 c: ctime
 S: check for growing size
 md5: md5 checksum
 sha1: sha1 checksum
 rmd160: rmd160 checksum
 tiger: tiger checksum
 R: p+i+n+u+g+s+m+c+md5
 L: p+i+n+u+g
 E: Empty group
 >: Growing logfile p+u+g+i+n+S

And also the following if you have mhash support enabled

crc32: crc32 checksum
 haval: haval checksum
 gost: gost checksum

EXAMPLES

/ R

This adds all files on your machine to the database. This is one line is a fully qualified configuration file.

!/dev

This ignores the /dev directory structure.

=/tmp

Only /tmp is taken into the database. None of its children are added.

All=p+i+n+u+g+s+m+c+a+md5+sha1+tiger+rmd160

This line defines group **All**. It has all attributes and all md checksum functions. If you absolutely want all digest functions then you should enable mhash support and add +crc32+haval+gost to the end of the definition for **All**. Mhash support can only be enabled at compile-time.

HINTS**=/foo R****/foo/bar R**

This config adds all files under /foo because they match to /foo, which is equivalent to /foo.* . What you probably want is:

=/foo\$ R**/foo/bar R**

Note that the following still works as expected because /foo is not recursed.

=/foo R The first is not allowed in AIDE. Use the latter instead.**/foo epug****/foo e+p+u+g****SEE ALSO****aide(1)** <http://www.cs.tut.fi/~rammer/aide/manual.html>**DISCLAIMER**

All trademarks are the property of their respective owners. No animals were harmed while making this webpage or this piece of software.