AIDE – Advanced Intrusion Detection Environment

- Kurzakte -

Installation	
• Paket aide aus Paketgruppe Produktivität/Sicherheit installiert nach /usr/bin/aide • Download der Quellen von http://www.cs.tut.fi/~rammer/aide.html Installation mit dem Dreisatz ./configure && make && make install	
Besondere Merkmale	
• gehört zu den Host-basierten Intrusion-Detection-Systemen (IDS), genauer: System Integrity Veryfier (SIV) • die komplette Installation (800 KB) inklusive Datenbank ist auf eine Diskette/CD auslagerbar: /usr/bin/aide, /etc/aide.conf und /var/lib/aide.db • kein Report per E-Mail, keine Verschlüsselung von Datenbank und Konfigurationsdatei	
Konfiguration des Servers und wichtige Datenbanken	
/etc/aide.conf	• Konfigurationsdatei sollte an einen sicheren Ort kopiert werden • enthält: - Parameter zur allgemeinen Einstellung anhand von Variablen (will man aide von einem sicheren Medium starten, kann man in der Konfigurationsdatei den Pfad zur aide.db auf ./aide.db ändern) - Festlegen von Attributgruppen - die wie zu überwachenden Dateien und Verzeichnisse (Selektionszeilen) dazu Objekt angeben, gefolgt von den Attributen, die AIDE überwachen soll
/var/lib/aide/aide.db.new	• die frisch erstellte Solldatenbank • /var/lib/aide/aide.db.new muss jetzt in /var/lib/aide/aide.db umbenannt werden, sofern das nicht in der Konfiguration geändert wurde.
/var/lib/aide/aide.db	• die aktuell genutzte Referenz-Datenbank • sollte gegen Manipulationen an einen sicheren Ort kopiert werden (CD)
Anwendung von Tripwire	
aide --init	• Initialisierung erstellt eine Referenz-Datenbank unter /var/lib/aide • systemkritische Dateien vorher manuell überprüfen (inetd.conf, passwd)
aide --check [-f ./aide.conf]	• Integritätstest des Systems (Abgleich reales Dateisystem mit Datenbank) • erzeugt eine Berichtausgabe auf der Konsole • sollte sinnvollerweise durch cron gestartet werden • ist die Default-Option: wird aide ohne Option gestartet, erfolgt ein Check • mit Parameter -f kann der Pfad zur Konfigurationsdatei angegeben werden
aide --update	• erzeugt eine aktualisierte Datenbank in /var/lib/aide/aide.db.new • Diese muss wieder umbenannt (/var/lib/aide/aide.db) und gesichert werden.
aide --compare	• Vergleich zweier Datenbanken, die in der Konfigurationsdatei mit den Angaben database= und database_new= definiert werden müssen.
aide --config=configdatei	• Liest die Konfiguration aus der angegebenen Datei statt aus /etc/aide.conf
aide --report_url=URL	• Gibt an, wohin AIDE seine Berichte ausliefern soll; Vorgabe ist stdout • mögliche URLs: stdout schreibt auf Standardausgabe stderr schreibt zusätzlich auf Standardfehlerausgabe stdin liest von Standardeingabe file://datei liest aus bzw. schreibt in die angegebene Datei fd:n liest aus bzw. schreibt in den angegebenen Filedeskriptor
aide --verbose=level	• Einstellen der Details beim Report von 0 – 255 • überschreibt den Wert in der Konfigurationsdatei • der Defaultwert ohne Angabe von --verbose ist 5 • Angabe von --verbose ohne Parameter: 20 • Maximalewert: 255
Dokumentation	
man: aide (1), aide.conf. (5)	

AIDE-Attribute zur Konfiguration der zu prüfenden Parameter	
Attribut	**Bedeutung**
p	Permissions (Zugriffsrechte)
i	Inode
n	Number of links (Anzahl der Hardlinks)
u	User
g	Group
s	Size (Größe)
m	Mtime (Modifikation des Datei-Inhalts)
a	Atime (Access, Zugriff)
c	Ctime (Change, Änderung der Inode-Information)
S	Growing Size (wachsende Größe)
md5	MD5-Checksumme von Ron Rivest
sha1	SHA1-Checksumme (Secure Hash Algorithm des NIST), der verbesserte SHA-Algorithmus
rmd160	RMD160-Checksumme (160 Bit, sehr sicher, RIPE Message Digest des europäischen RIPE-Projektes)
tiger	Tiger-Checksumme (bis 192 Bit)
crc32	CRC32-Checksumme
haval	Haval-Checksumme
gost	Gost-Checksumme (256 Bit aus Russland)
R	p+i+n+u+g+s+m+c+md5
L	p+i+n+u+g
E	Empty group (leere Auswahl)
>	Wachsendes Logfile (p+u+g+i+n+S)

Kommandofolge zur Initialsierung und Anwendung von AIDE

Erstellen einer einfachen Konfigurationsdatei zumm Test

```
linux:/etc # cat aide.conf
#
###  Parameter  ###
database=file:/var/lib/aide/aide.db
database_out=file:/var/lib/aide/aide.db.new
verbose=20
report_url=stdout
#
###  Gruppen von zu ueberpruefenden Attributen  ###
All=R+a+sha1+rmd160+tiger
Norm=s+n+b+md5+sha1+rmd160+tiger
R=p+i+n+u+g+s+m+c+md5
#
###  Folgende Verzeichnisse nicht ueberwachen  ###
!/dev
!/tmp
!/proc
!/usr/src
!/var/lib/aide   # ignore renamed aide.db.new to aide.db
!/var/run        # ignore pid-files
!/var/log/.*     # ignore the log dir it changes too often
!/var/spool/.*   # ignore spool dirs as they change too often
!/var/adm/utmp$  # ignore the file /var/adm/utmp
#
### testweise einige wichtige Verzeichnisse  ###
/etc  All-a      # check only permissions, inode, user and group for etc
/bin  Norm       # apply the custom rule to the files in bin
/sbin Norm       # apply the same custom rule to the files in sbin
/var  Norm       # apply the same custom rule to the files in var
```

Erstellen der Soll-Datenbank

```
linux:/etc # time aide --init
AIDE, version 0.10
### AIDE database initialized.

real    0m34.375s
user    0m16.005s
sys     0m0.835s

linux:/etc # du -h /var/lib/aide/aide.db.new
1.1M    /var/lib/aide/aide.db.new
```

Scharfschaltung durch einfaches Umbenennen

```
linux:/etc # cd
linux:~ # cd /var/lib/aide/
linux:/var/lib/aide # mv aide.db.new aide.db
```

Prüfen des Dateisystems auf Veränderungen im Vergleich zur Soll-Datenbank

```
linux:/var/lib/aide # aide --check
AIDE, version 0.10
### All files match AIDE database.  Looks okay!
```

testweises Verändern einer Datei

```
linux:/var/lib/aide # vi /etc/services

linux:/var/lib/aide # aide --check
AIDE found differences between database and filesystem!!
Start timestamp: 2005-07-21 14:51:35
Summary:
Total number of files=6170,added files=0,removed files=0,changed files=2

Changed files:
changed:/etc
changed:/etc/services
Detailed information about changes:

Directory: /etc
  Mtime    : 2005-07-21 14:48:07              , 2005-07-21 14:51:16
  Ctime    : 2005-07-21 14:48:07              , 2005-07-21 14:51:16

File: /etc/services
  Size     : 596413                           , 596411
  Mtime    : 2005-07-21 14:32:53              , 2005-07-21 14:51:16
  Ctime    : 2005-07-21 14:32:53              , 2005-07-21 14:51:16
  Inode    : 98432                            , 1115039
  MD5      : sgvRk/QqSh4Oe7KP6TmaEQ==         , Lh0CHJkaJc58g0VRymxs+A==
  SHA1     : lbH/UEvoQCJmH74Q070RfQuN+6g=     ,
  K/vIUt8Ak6m5q292SHurrWdaP8U=
  RMD160   : VKxbIQNBMqav9/rgjquMGJN6CZI=     ,
  fo8XlcaPHAeTmud1N3ZoY6y5Mxk=
  TIGER    : OKlHyU4md8IQ8Z/ywR2K+STTr8QuFxmt  ,
  dcCqUrZOK3iMCFVOqSOX24M0zFQsIx0s

linux:/var/lib/aide # aide --update
...

linux:/var/lib/aide # mv aide.db.new aide.db

linux:/var/lib/aide # aide --check
AIDE, version 0.10
### All files match AIDE database.  Looks okay!
```

suselinux:~ # cat /etc/aide.conf

```
#
#       SUSE-Beispielsdatei unter /etc/aide.conf
#
# Configuration parameters
database=file:/var/lib/aide/aide.db
database_out=file:/var/lib/aide/aide.db.new
verbose=1
report_url=stdout
warn_dead_symlinks=yes
#
# Custom rules
All             = R+a+sha1+rmd160+tiger              # von mir hinzugefügt
Binlib          = p+i+n+u+g+s+b+m+c+md5+sha1
ConfFiles       = p+i+n+u+g+s+b+m+c+md5+sha1
Logs            = p+i+n+u+g+S
Devices         = p+i+n+u+g+s+b+c+md5+sha1
Databases       = p+n+u+g
StaticDir       = p+i+n+u+g
ManPages        = p+i+n+u+g+s+b+m+c+md5+sha1
#
# Directories and files
#### Kernel, system map, etc.
/boot                                   Binlib
#### watch config files, but exclude, what changes at boot time, ...
!/etc/mtab
!/etc/lvm*
/etc                                    ConfFiles
#### Binaries
/bin                                    Binlib
/sbin                                   Binlib
#### Libraries
/lib                                    Binlib
#### Complete /usr and /opt
/usr                                    Binlib
/opt                                    Binlib
#### Log files
/var/log$                               StaticDir
#/var/log/aide/aide.log(.[0-9])?(.gz)?  Databases
#/var/log/aide/error.log(.[0-9])?(.gz)? Databases
#/var/log/setuid.changes(.[0-9])?(.gz)? Databases
/var/log                                Logs
#### Devices
!/dev/pts
/dev                                    Devices
#### Other miscellaneous files
/var/run$                               StaticDir
!/var/run
/var/lib                                Databases
#### Test only the directory when dealing with /proc
/proc$                                  StaticDir
!/proc
#### manpages can be trojaned, especially depending on *roff implementation
#/usr/man                               ManPages
#/usr/share/man                         ManPages
#/usr/local/man                         ManPages
#### check sources for modifications
#/usr/src                               L
#/usr/local/src                         L
#### Check headers for same
#/usr/include                           L
#/usr/local/include                     L
```