Программно-аппаратный комплекс доверенной загрузки «Блокхост-МДЗ»

Подсистема контроля целостности для Linux

Описание применения

Аннотация

Настоящий документ содержит описание применения подсистемы контроля целостности для Linux программно-аппаратного комплекса доверенной загрузки «Блокхост-МДЗ» (далее по тексту – ПАК «Блокхост-МДЗ»).

Содержание

1 Назначение подсистемы контроля целостности для Linux 4
2 Условия применения 4
3 Работа с эмулятором терминала 4
3.1 Запуск подсистемы 5
3.2 Настройки подсистемы 5
3.3 Работа со списком контролируемых файловых объектов 6
3.4 Виды контроля целостности файловых объектов 7
3.5 Запуск/остановка службы 8
3.6 Просмотр текущей версии 8
3.7 Получение справки о программе 8

1 Назначение подсистемы контроля целостности для Linux

Подсистема контроля целостности для Linux предназначена для проведения периодического/событийного контроля целостности файловых объектов и содержимого каталогов на рабочей станции, а также контроля целостности атрибутов файловых объектов.

Возможности подсистемы:

- формирование списка контролируемых файловых объектов. Подсистема контроля целостности предоставляет возможность постановки файлового объекта на контроль и снятия его с контроля;
- управление подсистемой контроля целостности, включающее:
  - запуск/остановку подсистемы;
  - выбор алгоритма подсчета контрольных сумм;
  - настройку Syslog-сервера;
  - изменение периодичности контроля;
- контроль целостности файловых объектов. Подсистема контроля целостности проводит периодический контроль целостности контролируемых файловых объектов, контроль целостности по событию, а также контроль целостности атрибутов файловых объектов.

2 Условия применения

Подсистема контроля целостности работает под управлением ОС Linux на платформе x86/x86-64.

Для вычисления контрольных сумм файловых объектов по алгоритму ГОСТ Р 34.11-94 должна быть установлена СКЗИ «КриптоПро CSP» (версия 3.6).

3 Работа с эмулятором терминала

Подсистема контроля целостности не имеет графического интерфейса. Работа с подсистемой ведется в режиме суперпользователя с помощью диалогового окна эмулятора терминала. Для работы с подсистемой контроля целостности для ОС Linux доступны следующие команды:

- «-start» – запуск службы контроля файлов Blokhost-MDZ;
- «-stop» - остановка службы контроля файлов Blokhost-MDZ;
- «-clear» – возвращение к начальному состоянию параметров (сброс настроек);
- «-add» – постановка файлов/каталогов на контроль;
- «-del» – удаление файлов/каталогов из списка контролируемых объектов;
- «-timegap» – установка периода контроля;
- «-syslogs» – задание ip-адресов syslog-серверов;
- «-hash» – выбор алгоритма расчета контрольных сумм добавляемых объектов;
- «-view-hash» – просмотр текущего алгоритма расчета контрольных сумм;
- «-view-timegap» – просмотр текущего периода контроля;
- «-view-syslogs» – просмотр текущих адресов syslog-серверов;
- «-view-files» – просмотр списка контролируемых объектов;
- «-version» – просмотр версии программы;
- «-help» – помощь – вывод списка команд.

Параметры команд, указанные в квадратных скобках [ ] далее по тексту, не являются обязательными.

3.1 Запуск подсистемы

Вызов подсистемы может быть осуществлен из эмулятора терминала вводом следующей команды: <*директория подсистемы*> # *./filecontrol*<*команда*>.

3.2 Настройки подсистемы

Настройка подсистемы контроля целостности выполняется в режиме суперпользователя.

3.2.1 Выбор алгоритма подсчета контрольных сумм

Для выбора алгоритма подсчета контрольных сумм необходимо ввести команду <*директория подсистемы*> # *./filecontrol -hash* <*algorithm*>.

Для подсчета контрольных сумм могут быть использованы следующие алгоритмы подсчета:

- MD5;
- GOST 34.11-94;
- SHA1;
- SHA224;
- SHA256;
- SHA384;
- SHA512;
- RIPEMD160;
- Whirlpool.

Например: /home/user/Desktop/blokhost-mdz #./filecontrol -hash md5.

При следующем добавлении файлов или каталогов подсчет их контрольных сумм будет проводиться по указанному алгоритму.

3.2.2 Периодичность контроля

Для того, чтобы задать периодичность проведения контроля целостности в диалоговом окне эмулятора терминала необходимо ввести команду <*директория подсистемы*> *# ./filecontrol –timegap* <HH:MM|HH> (где «HH» - часы, «MM» – минуты).

Контроль целостности будет проводиться с указанной периодичностью и при внесении изменений в контролируемые файлы на Syslog-сервер будет отправлено сообщение об изменении контролируемого файла.

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -timegap 00:10

3.2.3 Настройки Syslog-сервера

При обнаружении нарушения подсистема контроля целостности отправляет сообщения на Syslog-сервер.

Для настройки параметров Syslog-сервера в командной строке ввести команду <*директория подсистемы*>*./filecontrol –syslogs* <*address_list*>.

«address_list» - список адресов syslog-серверов в формате *IP:порт* (через двоеточие (:)). Если опустить указание номера порта, то по умолчанию будет использоваться порт 514. Если Syslog-серверов несколько, для каждого необходимо выполнить вышеперечисленные действия.

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -syslogs 192.168.78.24

3.2.4 Просмотр текущих настроек

Для просмотра выбранного алгоритма подсчета контрольных сумм необходимо ввести команду *<директория подсистемы> # ./filecontrol –view –hash.*

Для просмотра установленного периода контроля необходимо ввести команду *<директория подсистемы> # ./filecontrol –view-timegap.*

Для просмотра заданного адреса Syslog-сервера необходимо ввести команду *<директория подсистемы> # ./filecontrol –view-syslogs.*

3.2.5 Сброс настроек

Для возвращения к начальному состоянию параметров (сброса настроек) используется команда *<директория подсистемы> # ./filecontrol -clear <sysconf/syslogs/files>*, где:

- *«sysconf»* – сброс настроек алгоритма расчета контрольных сумм и периода контроля;
- *«syslogs»* – сброс ранее заданных адресов syslog-серверов;
- *«files»* – очистка списка контролируемых объектов.

Например: /home/user/Desktop/blokhost-mdz #./filecontrol -clear files.

3.3 Работа со списком контролируемых файловых объектов

В подсистеме существует возможность добавлять в список контролируемых объектов как отдельные файлы, так и каталоги с их содержимым.

3.3.1 Добавление файлов/каталогов в список контролируемых объектов

Для добавления файла в список необходимо ввести команду *<директория подсистемы> # ./filecontrol –add [-R] -check <event|period> [-hash <algorithm>] -files <file_list>*, где:

- *«-R»* – рекурсия. Используется только при постановке на контроль каталогов, для того, чтобы поставить на контроль все входящие в него подкаталоги;
- «*-check <event/period>»* - определяет политику контроля целостности поставленных на контроль объектов:
  - «*event*» – контроль по событию, при изменении объекта сообщение об этом сразу же поступает на syslog-сервер;
  - «*period*» – контроль производится через заданный период времени.
- «*-hash <algorithm>*» - задает алгоритм для расчета контрольных сумм поставленных на контроль файлов/каталогов. Если локальный алгоритм определен, то он заменяет глобальный алгоритм, определенный автономной командой –hash;
- *«-files <file_list>»* - список файлов/каталогов. Для добавления нескольких объектов в список в скобках указываются пути и имена файлов через точку с запятой (;).

Например:

/home/user/Desktop/blokhost-mdz # ./filecontrol -add -check event -hash md5 -files /home/user/Desktop/file.

/home/user/Desktop/blokhost-mdz # ./filecontrol -add -R -check event -hash md5 -files /home/user/Desktop/folder.

3.3.2 Удаление файлов/каталогов из списка контролируемых объектов

Для удаления файла из списка в эмуляторе терминала необходимо ввести команду *<директория подсистемы>./filecontrol –del [-R] –files <путь и имя файла>*, где:

- *«-R»* – рекурсия. Используется только при удалении каталогов из списка, для того, чтобы удалить все входящие в него подкаталоги;
- *«-files <file_list>»* - список файлов/каталогов, которые требуется удалить. Для удалении нескольких объектов в скобках указываются пути и имена файлов через точку с запятой (;).

Например:

/home/user/Desktop/blokhost-mdz # ./filecontrol -del -files /home/user/Desktop/file.

/home/user/Desktop/blokhost-mdz # ./filecontrol -del -r -files /home/user/Desktop/folder.

3.3.3 Просмотр списка контролируемых объектов

Список объектов, поставленных на контроль, можно посмотреть с использованием команды *<директория подсистемы> # ./filecontrol -view-files [-R] -shown-info <opt_list> [-files <file_list>],* где:

- «*-R*» – указывается только для каталогов, когда нужно показать все файлы в каталоге, включая подкаталоги;
- «*-shown-info <opt_list>»* - «*opt_list*» – список опций. Могут быть использованы следующие опции:
  - «*attr*» – показать только атрибуты файла;
  - «*hash*» – показать только контрольные суммы файлов;
- «*-files <file_list>»* - список файлов/каталогов, информацию о которых нужно получить (при указании нескольких объектов они должны быть отделены друг от друга точкой с запятой (;)).

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -view-files -R -shown-info attr.

3.4 Виды контроля целостности файловых объектов

3.4.1 Проведение контроля целостности по событию

Для проведения контроля по событию необходимо добавить объект на контроль в соответствии с пунктом 3.3.1, указав политику контроля целостности «*event*».

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -add -check event -hash md5 -files /home/user/Desktop/file.

После изменения поставленного на контроль объекта на Syslog-сервере появится сообщение об изменении контролируемого файла следующего вида:

Mar 28 10:30:29 linux-xu7q Blokhost-MDZ: attributes of file '/home/user/Desktop/file.txt' had been changed :: OLD: size=7, mtime=Mar 17 12:20, ctime=Mar 17 12:20; NEW: size=24, mtime=Mar 28 10:30, ctime=Mar 28 10:30.

3.4.2 Проведение периодического контроля

Для проведения периодического контроля целостности необходимо:

1) установить период контроля с помощью команды *–timegap* < HH:MM|HH >*;*

2) добавить контролируемые объекты в список в соответствии с пунктом 3.3.1, указав в политике контроля целостности параметр «*period*».

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -add -check period -hash md5 -files /home/user/Desktop/file.

После изменения поставленного на контроль файла через указанный период на Syslog-сервере появится сообщение об изменении контролируемого файла следующего вида:

Mar 28 10:37:16 linux-xu7q Blokhost-MDZ: attributes of file '/home/user/Desktop/file.txt' had been changed :: OLD: size=24, mtime=Mar 28 10:30, ctime=Mar 28 10:30; NEW: size=32, mtime=Mar 28 10:36, ctime=Mar 28 10:36.

3.4.3 Проведение контроля атрибутов файла

Для проведения контроля целостности атрибутов файла необходимо добавить объект на контроль в соответствии с пунктом 3.3.1, указав в политике контроля целостности параметр «*event*».

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol -add -check event -hash md5 -files /home/user/Desktop/file.

После изменения атрибутов контролируемого файла на Syslog-сервере появится сообщение следующего вида:

Mar 28 12:34:52 linux-xu7q Blokhost-MDZ: attributes of file '/home/user/Desktop/file.txt' had been changed :: OLD: mode=-rw-r--r--, uid=1000, size=24, mtime=Mar 28 10:30, ctime=Mar 28 10:30; NEW: mode=-rwxrwxrwx, uid=0, size=32, mtime=Mar 28 10:36, ctime=Mar 28 12:31.

3.5 Запуск/остановка службы

Подсистема контроля целостности позволяет осуществлять запуск и остановку службы контроля целостности файлов Blokhost-MDZ, для чего используются команды:

- *<директория подсистемы> # ./filecontro l –start;*
- *<директория подсистемы> # ./filecontrol –stop.*
  Например: //home/user/Desktop/blokhost-mdz # ./filecontrol –start.

3.6 Просмотр текущей версии

Для просмотра информации о версии программы используется команда *<директория подсистемы># ./filecontrol –version.*

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol –version.

3.7 Получение справки о программе

Для получения справки по программе используется команда *<директория подсистемы> # ./filecontrol –help.*

Например: /home/user/Desktop/blokhost-mdz # ./filecontrol –help.