

- ◆ let's do some attack simulation against some file that contains important information (let's say, it is stored in the linux server)

```

root@LinuxSRV:~#
[root@LinuxSRV ~]# pwd
/root
[root@LinuxSRV ~]# ls -ltr
total 8
-rw-----. 1 root root 1388 Jan 31 13:40 anaconda-ks.cfg
-rw-r--r--. 1 root root 103 Apr 11 11:57 VIP_File.txt
[root@LinuxSRV ~]# cat VIP_File.txt
This file contains our trade secrets

Use this equation to estimate the k units per month

x3+y3+z3=k

```

- ◆ lets assume **VIP\_File.txt** file contains some trade secret for one company
- ◆ so basically we need to have a way or some capability to detect if the file has been tampered with
- ◆ previously we have installed windows agent, here we will do the linux agent installation, this will allow us to enable FIM (File Integrity Monitoring) capability where we can detect such attack.
- ◆ thanks to FortiSIEM which comes with built in rules that can detect or check for events coming from the FortiSIEM agent where some files has been tampered with or some attributes has been changed in some file system.
- ◆ first thing is to install the FortiSIEM linux agent on linux server

## Linux Agent Installation

### Prerequisites

- 1/ OS supported: CentOS/RHEL>7.4 and other linux flavors
- 2/ curl>7.19.7 & nss>3.36.0 otherwise >> yum update -y nss curl libcurl
- 3/ validate rsyslog >> systemctl status rsyslog.service >> if not running >> systemctl start rsyslog.service
- 4/ Make sure timezone is ok on the Linux machine >> timedatectl set-timezone Asia/Qatar

5/ The following packages must be installed (yum install <package\_name>) before FortiSIEM Linux Agents can run on CentOS/RHEL:

```
libcap  
audit  
audispd-plugins  
rsyslog  
logrotate
```

If SELinux is enabled (sestatus), then the following packages also must be installed:

```
policycoreutils  
libselinux-utils  
setools-console
```

## Install/Start/Configure the Agent

---

1/ Download the Linux installation script from Fortinet Support website support.fortinet.com and upload it using WinSCP

2/ chmod +x fortisiem-linux-agent-installer-6.6.0.1633.sh

3/ Run the command: bash fortisiem-linux-agent-installer-<VERSION>.sh -s <SUPER\_IP> -i <ORG\_ID> -o <ORG\_NAME> -u <AGENT\_USER> -p <AGENT\_PWD> -n <HOST\_NAME>

```
bash fortisiem-linux-agent-installer-6.6.0.1633.sh -s 192.168.100.155 -i  
1 -o super -u lnxusr -p P@ssword@123 -n LinuxSRV
```

4/ Start the agent: /usr/bin/sh -c /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent &

5/ Define the template and assign to host

6/ If File Integrity monitoring is chosen, validate the SELinux context  
ls -Z >> validate SE context is var\_log\_t >> or change >> chcon  
system\_u:object\_r:var\_log\_t:s0 VIP\_File.txt

## Log Rotation

---

[https://docs.fortinet.com/document/fortisiem/6.6.3/linux-agent-installation-guide/201446/fortisiem-linux-agent#Log\\_Rotating\\_var\\_log\\_messages\\_to\\_Prevent\\_Filling\\_Up\\_the\\_Root\\_Disk](https://docs.fortinet.com/document/fortisiem/6.6.3/linux-agent-installation-guide/201446/fortisiem-linux-agent#Log_Rotating_var_log_messages_to_Prevent_Filling_Up_the_Root_Disk)

## UnInstall the Agent

---

/opt/fortinet/fortisiem/linux-agent/bin/fortisiem-linux-agent-uninstall.sh

## Sources

---

<https://docs.fortinet.com/document/fortisiem/6.7.3/linux-agent->

```
installation-guide/201446/fortisiem-linux-agent  
https://help.fortinet.com/fsiem/6-6-0/Online-Help/HTML5\_Help/Configuring\_Linux\_Agent.htm  
https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_linux/7/html/selinux\_users\_and\_administrators\_guide/sec-enhanced\_linux-working\_with\_selinux-selinux\_contexts\_labeling\_files  
https://unix.stackexchange.com/questions/79311/configuring-selinux-to-allow-logging-to-a-file-thats-outside-var-log  
https://docs.fortinet.com/document/fortisiem/6.6.3/linux-agent-installation-guide/201446/fortisiem-linux-agent#Managing
```

- ◆ check the prerequisites

root@LinuxSRV:/tmp/fortisiem-linux-agent

```
[root@LinuxSRV fortisiem-linux-agent]# pwd  
/tmp/fortisiem-linux-agent  
[root@LinuxSRV fortisiem-linux-agent]# ls -ltr  
total 68364  
-rwxr-xr-x. 1 root root 69997285 Jul 20 2022 fortisiem-linux-agent-installer-6.6.0.1633.sh  
-rw-r--r--. 1 root root 103 Apr 26 09:14 deleted_bkp  
[root@LinuxSRV fortisiem-linux-agent]# cat /etc/redhat-release  
CentOS Linux release 8.1.1911 (Core)  
[root@LinuxSRV fortisiem-linux-agent]# rpm -qa curl  
curl-7.61.1-11.el8.x86_64  
[root@LinuxSRV fortisiem-linux-agent]# rpm -qa nss  
nss-3.44.0-8.el8.x86_64  
[root@LinuxSRV fortisiem-linux-agent]#
```

root@LinuxSRV:/tmp/fortisiem-linux-agent

```
ns-3.44.0-8.el8.x86_64  
[root@LinuxSRV fortisiem-linux-agent]# systemctl status rsyslog.service  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)  
   Active: active (running) since Wed 2023-04-26 10:34:40 +03; 15min ago  
     Docs: man:rsyslogd(8)  
           http://www.rsyslog.com/doc/  
 Main PID: 9086 (rsyslogd)  
    Tasks: 4 (limit: 4879)  
   Memory: 1.8M  
    CGroup: /system.slice/rsyslog.service  
           └─9086 /usr/sbin/rsyslogd -  
  
Apr 26 10:34:40 LinuxSRV systemd[1]: Starting System Logging Service...  
Apr 26 10:34:40 LinuxSRV systemd[1]: Started System Logging Service.  
Apr 26 10:34:40 LinuxSRV rsyslogd[9086]: environment variable TZ is not set, auto correcting this to TZ=/etc/localtime [v8.37.0-13.el8 try http://www.rsyslog.com/e/2442 ]  
Apr 26 10:34:40 LinuxSRV rsyslogd[9086]: [origin software="rsyslogd" swVersion="8.37.0-13.el8" x-pid="9086" x-info="http://www.rsyslog.com"] start  
[root@LinuxSRV fortisiem-linux-agent]#
```

- ◆ also check if SELinux is enabled (sestatus)

```
[root@LinuxSRV fortisiem-linux-agent]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:    actual (secure)
Max kernel policy version:     31
[root@LinuxSRV fortisiem-linux-agent]#
```

- ◆ while installing the linux agent, we need to create the agent user in the **FortiSIEM > CMDB**  
**> Users > New**
  - ◆ make sure **System Admin** checkbox is checked and inside that select **Agent Admin** and put username and password
- ◆ retrieve server name from the linux server and then install

```
[root@LinuxSRV fortisiem-linux-agent]# ls -ltr
total 68364
-rwxr--xr-x. 1 root root 69997285 Jul 20 2022 fortisiem-linux-agent-installer-6.6.0.1633.sh
-rw-r--r--. 1 root root 103 Apr 26 09:14 deleted.bkp
[root@LinuxSRV fortisiem-linux-agent]# bash fortisiem-linux-agent-installer-6.6.0.1633.sh -s 192.168.100.155 -i 1 -o super -u lnxusr -p P@ssword@123 -n LinuxSRV
Checking Connectivity to Server ... 192.168.100.155
Supervisor at 192.168.100.155 is reachable. Continuing with installation...
Agent parameters validated successfully
SUPER_IP:192.168.100.155
CUSTOMER_ID:1
CUSTOMER_NAME:super
AGENT_REG_USERNAME:lnxusr
AGENT_REG_PASSWORD:P@ssword@123
PROXY_SERVER_IP:
PROXY_SERVER_PORT:
SSL_VERIFY_PEER:false
SSL_CA_CERT_FILE:/etc/pki/tls/certs/ca-bundle.crt
HOST_NAME:LinuxSRV
SSL_CA_CERT_PATH:
Executing command systemctl start fortisiem-linux-agent.service
Executing command systemctl enable fortisiem-linux-agent.service
Created symlink /etc/systemd/system/multi-user.target.wants/fortisiem-linux-agent.service → /etc/systemd/system/fortisiem-linux-agent.service.
Executing command systemctl daemon-reload
service fortisiem-linux-agent status...
Redirecting to /bin/systemctl status fortisiem-linux-agent.service
● fortisiem-linux-agent.service - FortiSIEM Linux Agent daemon
   Loaded: loaded (/etc/systemd/system/fortisiem-linux-agent.service; enabled; vendor preset: disabled)
   Active: activating (auto-restart) (Result: exit-code) since Wed 2023-04-26 10:56:19 +03; 88ms ago
     Main PID: 10051 (code=exited, status=1/FAILURE)
       Tasks: 0 (limit: 4879)
      Memory: 0B
        CGroup: /system.slice/fortisiem-linux-agent.service
INSTALLATION SUCCESS, but service did not start.
Please check if the agent registration username or password is incorrect
Also please check for errors in the agent log here: /opt/fortinet/fortisiem/linux-agent/log/phoenix.log
[root@LinuxSRV fortisiem-linux-agent]#
```

- ◆ to start the service

```
/usr/bin/sh -c /opt/fortinet/fortisiem/linux-agent/bin/phLinuxAgent &
```

## Note: info about license usage and regarding the agents

- ◆ you will see separate count for number of **Agents** and number of **UEBA**
- ◆ actually **UEBA** is a feature inside the **Agent**
  - ◆ it's a kernel level component that is being installed along with the same agent that you install

The screenshot shows the FortiSIEM Admin interface under the License tab. It displays a table of license usage details. The table has columns for Attribute, Value, and Expiry. Two rows, 'Agents' and 'UEBA', are highlighted with a red box and have a yellow background. The 'Agents' row shows a value of 100 and an expiry of May 15, 2023. The 'UEBA' row shows a value of 500 and an expiry of May 15, 2023.

Attribute	Value	Expiry
Devices	500	May 15, 2023
Endpoint Devices	N/A	N/A
Additional EPS	N/A	N/A
Total EPS	5000	May 15, 2023
Agents	100	May 15, 2023
UEBA	500	May 15, 2023
IOC Service	Valid	May 15, 2023
Maintenance and Support	Valid	May 15, 2023

- ◆ here we can see the usage.

The screenshot shows the FortiSIEM Admin interface under the Usage tab. It displays a summary of agent counts. The 'Agent Usage' section is active, showing counts for Linux, Windows, and Total agents. The 'UEBA' count is highlighted with a red box and has a yellow background. The total count is 1.

Category	Count
Linux Agent	0
Windows Agent	1
Total	1
UEBA	1

- ◆ why we have UEBA because, in the installing the windows agent we have checked the UEBA

The screenshot shows the FortiSIEM interface for editing a Windows Agent Monitor Template. The 'Edit Windows Agent Monitor Template' title is at the top. Below it is a navigation bar with tabs: Generic, Event, UEBA, User Log, FIM, Change, and Script. The 'UEBA' tab is active and highlighted with a red box. At the bottom, there is a note: 'UEBA:  (Requires UEBA Telemetry License)'.

- ◆ this is how you can track your license usage
- ◆ now after successful installation of linux agent, its showing as **Registered**

The screenshot shows the FortiSIEM interface under the 'Agent Health' tab. It displays a table of agents with columns: Name, IP Address, Device Type, Agent Type, Agent Version, Agent Status, Event Status, and Monitor Status. Two agents are listed: 'LinuxSRV' (IP 192.168.100.175) and 'WindowsDemo' (IP 192.168.18.11). The 'Agent Status' column shows 'Registered' for both, with the word highlighted in red. The 'Event Status' and 'Monitor Status' columns also show 'Registered'.

- ◆ to make it active (**Running Active**), we need to define the template

The screenshot shows the 'Add Linux Agent Monitor Template' dialog box. The 'Syslog' tab is selected. The configuration table has rows for facility levels (kern, user, mail, daemon, auth, syslog, lpr, news, uucp, authpriv) and severity levels (All, Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug). In the 'auth' row, the 'Info' checkbox is checked. The 'Save' and 'Cancel' buttons are at the bottom. A red box highlights the 'Linux Agent' tab in the top right corner of the dialog.

- ◆ in our case, we need to monitor important file (e.g., **VIP\_File.txt** ), include this in FIM
  - ◆ **Push Files** will push the metadata into FortiSIEM (actually stored in SVN database)

Add Linux Agent Monitor Template

Include File/Directory:

Exclude File/Directory:

Delimiter:

File Encoding:

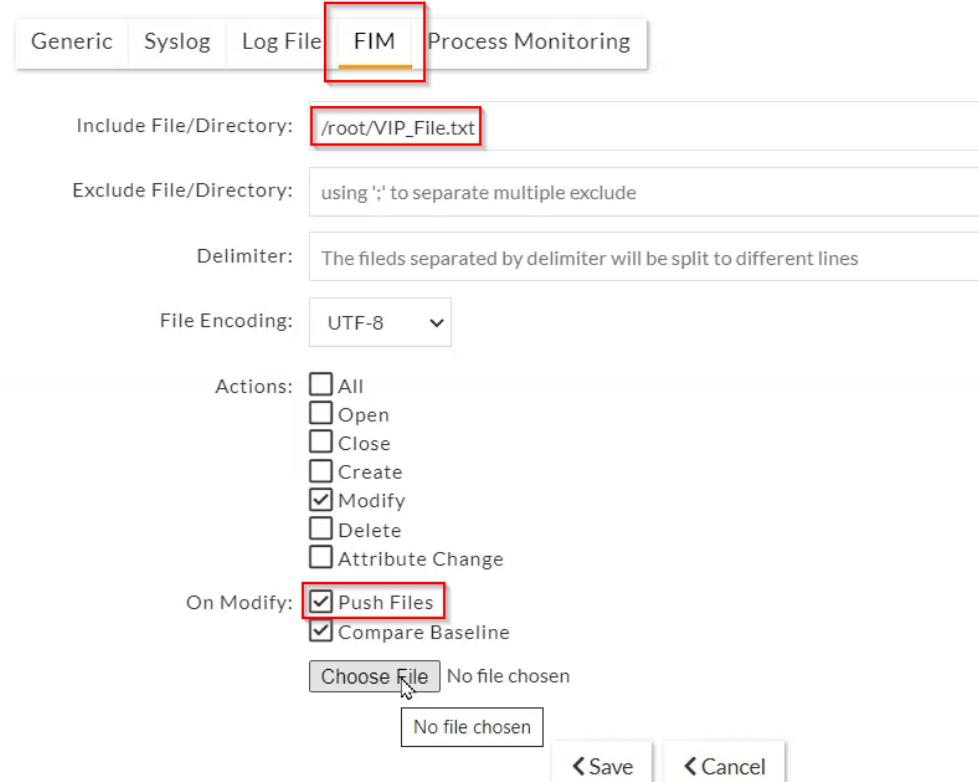
Actions:

- All
- Open
- Close
- Create
- Modify
- Delete
- Attribute Change

On Modify:

- Push Files
- Compare Baseline

No file chosen



- ◆ then we need to associate this template into some host

Host To Template Associations

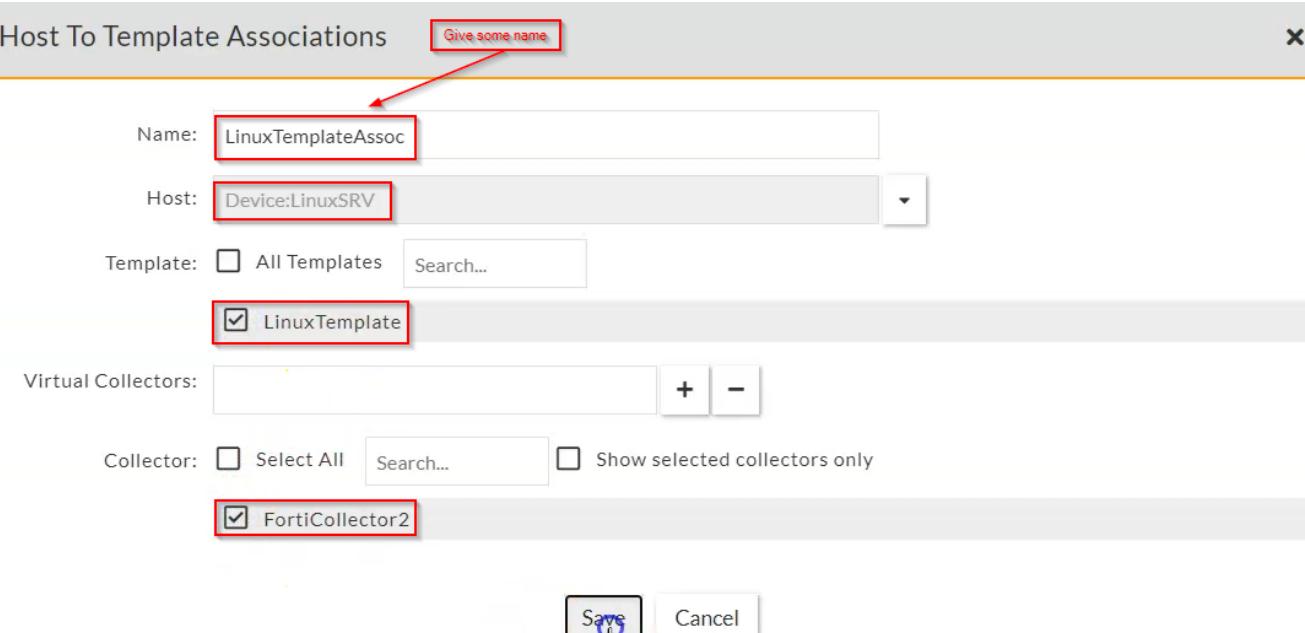
Name:

Host:

Template:  All Templates   
 LinuxTemplate

Virtual Collectors:

Collector:  Select All   Show selected collectors only  
 FortiCollector2



- ◆ and then apply, and then you can see **Running Active** in Health section in ADMIN panel
- ◆ let's check what are the built-in rules that can be useful to detect the modification attempt

**FortiSIEM**

Dashboard Analytics Incidents Cases CMDB Resources Tasks Admin

Reports Rules Machine Learning Jobs Watch Lists Lookup Tables Osquery Connectors Playbooks Remediations Malware Domains Malware IPs Malware Hash Malware Processes Malware URLs Anonymity Network Country Groups Default Password Event Types Networks Protocols

Resources > Rules

New Edit Delete More

Search: FIM

Active	Severity	Name	Description	Tactics	Technique	Scope	Data Source	Detection Tech...	Test Status	Exceptions	Ev...
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux Directory Ownership or Permission Changed	FortSIEM Linux Agent FIM detected that a directory ownership or permission changed	Impact, Defense Evasion	Data Manipulation: Stored Data Manipulation [T1565.001], File and Directory Permissions Modification: Linux and Unix File and Directory Permissions Modification [T1222.002]	System	Linux FIM Via FortSIEM Agent	Correlation			
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux File Changed From Baseline	FortSIEM Linux Agent FIM detected that a file changed from its baseline	Impact, Defense Evasion	Data Manipulation: Stored Data Manipulation [T1565.001], Indicator Removal on Host: File Deletion [T1070.004]	System	Linux FIM Via FortSIEM Agent	Correlation			
<input checked="" type="checkbox"/>	7 - MEDIUM	(s) Agent FIM: Linux File Content Modified	Detects that a user modified either the content or the attributes of a file or directory	Impact, Defense Evasion	Data Manipulation: Stored Data Manipulation [T1565.001], Indicator Removal on Host: File Deletion [T1070.004]	System	Any Device Agentless FIM via SSH	Correlation			

Summary Test Results Auto expand

- ◆ let's see what exact rule will be triggered when we try to modify the file

**FortiSIEM**

DASHBOARD ANALYTICS INCIDENTS CASES CMDB RESOURCES TASKS ADMIN

Actions [1] Raw Messages

Event Type != PH\_DEV\_MON\_PING\_STAT

Run

Raw Messages - Last 10 Minutes

Indicator Chart for COUNT(Matched Events)

Show Event Type Wrap Raw Events Execute Playbook Run Connector

Event Receive Time Reporting IP Event Type Event Name Raw Event Log

Apr 26 2023, 11:17:56 AM	192.168.100.175	FSM_LINUX_FILE MODIFY	A watched file or a file within a watched directory was written to	Wed Apr 26 11:17:42 2023 LinuxSRV:[FSM_LINUX_FILE MODIFY]:[objectTy...]
Apr 26 2023, 11:17:56 AM	192.168.100.175	FSM_LINUX_FILE MODIFY	A watched file or a file within a watched directory was written to	A watched file or a file within a watched directory was written to
Apr 26 2023, 11:17:16 AM	192.168.100.175	Generic_Linux_Generic	Generic_Linux_Generic	Wed Apr 26 11:17:07 2023 LinuxSRV:[user]=unknown
Apr 26 2023, 11:09:17 AM	192.168.100.175	Generic_Linux_Generic	Generic_Linux_Generic	Wed Apr 26 11:09:02 2023 LinuxSRV:[user]=root

Copyright © 2022 Fortinet, Inc. All rights reserved.

FortiSIEM 6.6.0.1633

- ◆ you can view detailed event in **Event Details**

## Event Details



Wed Apr 26 11:17:42 2023 LinuxSRV: [FSM\_LINUX\_FILE MODIFY]: [objectType]=Directory, [objectName]=/root/, [objectAction]=MODIFY, [targetObjType]=File, [targetObjName]=/root/VIP\_File.txt, [hashCode]=13d3fa53e7a6d74094d6e16dbbecfd68, [hashAlgo]=md5, [user]=root

Lines: 33

Display	Filter	Item	Value
<input type="checkbox"/>	<input type="checkbox"/>	Collector ID	10001
<input type="checkbox"/>	<input type="checkbox"/>	Count	1
<input type="checkbox"/>	<input type="checkbox"/>	Device Time	Apr 26 2023, 11:17:42 AM
<input type="checkbox"/>	<input type="checkbox"/>	Event ID	4489666616032018548
<input type="checkbox"/>	<input type="checkbox"/>	Event Name	A watched file or a file within ...
<input type="checkbox"/>	<input type="checkbox"/>	Event Parse Status	1
<input type="checkbox"/>	<input type="checkbox"/>	Event Parser Name	LinuxInotifyParser
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Event Receive Time	Apr 26 2023, 11:17:56 AM
<input type="checkbox"/>	<input type="checkbox"/>	Event Rule Trigger	1
<input type="checkbox"/>	<input type="checkbox"/>	Event Severity	5

- ◆ you can also view details in **INCIDENTS** page in overview section

## Note:

- ◆ One important capability of monitoring is that the ability to see the differences between the files being modified
- ◆ metadata of the files being modified is updated or uploaded to the SVN databases of the supervisors. so you can have the multiple revisions of the same file and you can compare between these revisions and pinpoint the changes that have occurred.
- ◆ you can also compare the metadata of the modified file against a master image. so you can also know what has been changed. to check this you have to check the record created of the host inside the CMDB database, from here you can check the file being modified in that host

- ◆ here we can see the modification in metadata. first we tried with file itself, the the file path
- ◆ you can select both and see the difference (useful when comparing two same files)

## File Diff



Rev #1 Apr 26 2023, 11:04:13 AM /root/VIP_File.txt		Rev #2 Apr 26 2023, 12:25:29 PM /root/VIP_File.txt	
1	----- File Metadata Begin -----	1	----- File Metadata Begin -----
2	OWNER=root	2	OWNER=root
3	GROUP=root	3	GROUP=root
4	PERMISSION=USER: "OWNER", PERMIT: "READ,WRITE,"	4	PERMISSION=USER: "OWNER", PERMIT: "READ,WRITE,"
5	PERMISSION=GROUP: "MEMBER", PERMIT: "READ"	5	PERMISSION=GROUP: "MEMBER", PERMIT: "READ"
6	PERMISSION=GROUP: "OTHER", PERMIT: "READ,"	6	PERMISSION=GROUP: "OTHER", PERMIT: "READ,"
7	FILEPATH=/root/VIP_File.txt	7	FILEPATH=/root/VIP_File.txt
8	HASHCODE=80ce168f9b01063ff310cb20605efc3a	8	HASHCODE=5fb690dc2c9497534401d7605db1135c
9	HASHALGO=MD5	9	HASHALGO=MD5
10	MODIFIED_TIME=2023-04-26T08:04:10Z	10	MODIFIED_TIME=2023-04-26T09:25:20Z
11	----- File Metadata End -----	11	----- File Metadata End -----
12	This file contains our trade secrets	12	This file contains our trade secrets
13		13	
14	Use this equation to estimate the k units per month	14	Use this equation to estimate the k units per month
15		15	
16	$x^3+y^3+z^3=k$	16	$4^*x^3+3^*y^3+2^*z^3=k$
17		17	
18		18	
19		19	

[Top](#)[Bottom](#)[Previous](#)[Next](#)[Close](#)

- ◆ this is the importance of FIM (File Integrity Monitoring)