THALES

Learn Mode Tool

CTE V7.6.0

Learn Mode Tool

The Learn Mode Policy Builder (`lmpb`) is an OpenSource Python-based tool for processing the CipherTrust Transparent Encryption Learn Mode audit logs and generating security policies. Learn Mode allows access to guarded paths while logging access details. This tool helps administrators understand the gap between the current policy and the required policy and suggests corrective changes. The CipherTrust Manager and file system administrators are advised to review the changes before pushing them to CipherTrust Manager.

> **Note**
>
> This is an unsupported tool. Users are free submit request for enhancements and bugs, but Thales will not treat them as escalations.

Prerequisite

To collect logs that can be processed by the Learn Mode tool, enable the Learn Mode toggle on the CipherTrust Manager GUI while creating a policy.

Using the Learn Mode Tool

The Tool is available from the Thales site CipherTrust Transparent Encryption Git repository.

After you have the logs for Learn Mode, proceed as follows:

1. Clone the CipherTrust Transparent Encryption Git repository.

   ```
   git clone https://github.com/thalescpl-io/
   CipherTrust_Transparent_Encryption.git
   ```

2. Navigate to the `learn-mode-policy-builder` directory.

   ```
   cd CipherTrust_Transparent_Encryption/tools/learn-mode-policy-bui
   lder
   ```

3. View the common commands.

```
./lmpb -h
```

Sample Output

```
usage: lmpb [-h] [--logdir LOGDIR] {log,policy} ...

positional arguments:
  {log,policy}
    log              cte learn mode logs
    policy           learn mode policy updates

options:
  -h, --help         show this help message and exit
  --logdir LOGDIR    log directory, defaults to /var/log/vormetric
```

Log Related Commands

```
    ./lmpb --logdir /home/logs/logs/ubu0/ log
```

Sample Output

```
positional arguments:
  {status,process,report}
    status                logs status
    process               process logs
    report                print log report in text format

options:
  -h, --help              show this help message and exit
```

View the log status:

```
./lmpb --logdir /home/logs/logs/ubu0/ log status
```

- If unprocessed logs are present, output displays as follows:

  Sample Output

```
Found 181 log files in /home/logs/logs/ubu0/ with unprocessed
entries.
Total size of unprocessed entries is 326.62 MB
```

- If all log files are already processed, output displays as follows:

  Sample Output

```
No new log entries in /home/logs/logs/ubu0/ since Mon Dec  5
17:34:39 2022
```

- For processing the unprocessed log files, run the command:

```
./lmpb --logdir /home/logs/logs/ubu0/ log process
```

  Sample Output

```
Successfully parsed all log files
Other log entries: 9, saved to /tmp/lmskip.340576
Log output saved as JSON at /home/logs/logs/ubu0/output.json
```

- Input the `output.json` file to Splunk to visualize the data.

```
cat /home/logs/logs/ubu0/output.json | nc 10.171.56.220 6666
```

  In the example above, the SPLUNK server is configured to listen on port `6666` for `json_no_timestamp` events. The IP address `10.171.56.220` is an example.

- For viewing the log report:

```
./lmpb --logdir /home/logs/logs/ubu0/ log report
```

  Sample Output

  The output will show all processes, accesses performed by them, and the directories over which they have been performed.

```
    Process: [ /sdb/anom/vtebuild/
_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/build/env/linux/
5.4.0-48-generic/build/scripts/genksyms/genksyms ]
    Access:  [ write_app read_file_sec_attr read_attr ]
    Files/dirs: 20
    ---------------
    1 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-
generic/crypto/sha2/.tmp_sha256.ver
    2 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-
generic/vmcore/cfg/.tmp_vm_cfg_upd.ver
    3 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-
generic/vmcore/cfg/.tmp_vm_cfg.ver
    ...
    19 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-
generic/vmcore/common/.tmp_hexbin.ver
    20 /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-
generic/vmcore/ktctl/.tmp_vm_tc.ver
```

After the logs are processed by the Learn Mode policy builder tools, the following policy related commands can be run to list the existing policies or show updates recommended by the tool.

Policy Related Commands

```
./lmpb --logdir /home/logs/logs/ubu0/ policy
```

Sample Output

```
positional arguments:
  {list,show,upload}
    list                  list policies with learn mode updates
    show                  show learn mode policy updates
    upload                upload learn mode policy to CM


options:
  -h, --help            show this help message and exit
```

- List the policies with Learn Mode updates:

  ```
  ./lmpb --logdir /home/logs/logs/ubu0/ policy list
  ```

  Sample Output

```
Policies with learn mode updates:

audit
```

- Show Learn Mode policy updates:

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show
```

Sample Output

```
User sets:
  audit-uset-0
    [ audit ]
  audit-root-uset-1
    [ root ]

Process sets:
  audit-group-pset-0
    [ /sdb/anom/vtebuild/_obj_pem_64_perf_vor_ulinux_ubuntu20/mk/generate_messages_h.pl
    /usr/bin/dh_installdeb /usr/bin/dh_testroot /usr/lib/rpm/check-files /usr/lib/gcc/x86_64-linux-gnu/9/collect2 /usr/bin/ar /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/build/env/linux/5.4.0-48-generic/build/scripts/mod/modpost /usr/bin/make /bin/gzip /usr/bin/fakeroot
    ...]

  audit-group-pset-1
    [ /bin/mount /bin/df /bin/chmod /usr/bin/make /bin/bash /bin/sh /usr/bin/fakeroot /usr/bin/updatedb.mlocate /bin/ls ]

Resource sets:
  audit-rset-0
    [ /sdb/anom* ]

Security rules:
  Rule 0
    User set     audit-root-uset-1
    Process set  audit-group-pset-1
    Resource set audit-rset-0
    Action       d_chg_att,d_rd_att,d_rd_sec,f_rd,d_rd
    Effect       permit,applykey
  Rule 1
    User set     audit-uset-0
    Process set  audit-group-pset-0
    Resource set audit-rset-0
    Action
f_ren,d_chg_att,f_rm,d_rmdir,f_cre,d_rd_att,f_chg_sec,write,f_rd_
sec,d_rd_sec,f_rd_att,f_chg_att,f_wr,f_wr_app,f_rd,d_mkdir,d_rd
    Effect       permit,applykey
```

- Policies can be viewed based on users or processes. By default, it is user-based.

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show --type user
```

- The output of policy show in this case will be sorted, based on user sets. This is the default setting for policy show command.

```
./lmpb --logdir /home/logs/logs/ubu0/ policy show --type process
```

- The output of policy show in this case will be sorted, based on process sets.

Sample Output

```
Learn mode updates for policy audit:

User sets:
  audit-uset-0
    [ uset ]
  audit-root-uset-1
    [ root ]

Process sets:
…
  audit-cc1-pset-10
    [ /usr/lib/gcc/x86_64-linux-gnu/9/cc1 ]
  audit-fixdep-pset-11
```

```
    [ /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/build/env/linux/5.4.0-48-generic/build/scripts/basic/fixdep ]
…
Resource sets:
…
  audit-rset-10
    [ /sdb/anom/vtebuild/fspem* ]
  audit-rset-11
    [ /sdb/anom/vtebuild/_obj_fspem_64_perf_vor_klinux_5.4.0-48-generic/agent* ]
…
Security rules:
…
  Rule 10
    User set     audit-uset-0
    Process set  audit-which-pset-26
    Resource set audit-rset-2
    Action       d_rd_att
    Effect       permit,applykey
  Rule 11
    User set     audit-root-uset-1
    Process set  audit-ls-pset-57
    Resource set audit-rset-0
    Action       d_rd_att,d_rd,d_rd_sec
    Effect       permit,applykey
…
```

Uploading Policy to CipherTrust Manager

- To upload the policy to the CipherTrust Manager, run the command:

```
./lmpb --logdir /home/logs/logs/ora policy upload --policy-name LEARNMODE --type user --upload-name learn-mode-policy --cmaddr IP-ADDR-OF-CM --username admin --password PASSWORD
```

The above command will upload a policy to the CipherTrust Manager with modifications on top of the original policy suggested by the Learn Mode policy builder tool. Note that the above command will fail if the original policy is not found on the specified CipherTrust Manager.

Support Contacts

If you encounter a problem while installing, registering, or operating the product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at Thales Customer Support, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

Tip

You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the REGISTER link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support@Thales.com.