CFToolkit
New tooling in CFEngine 3.10, 3.12, and beyond

Ole Herman Schumacher Elgesem
Lead Developer, CFEngine

Agenda

1. Introduction
2. cf-net
3. cf-remote
4. cf-check
5. cf-policy-upgrade

CFEngine

Security - Fewer dependencies means fewer vulnerabilities

Stability - Small and mature code base means increased stability

Speed - Client written in C, executes in seconds, not minutes

Scale - Cheap and efficient scaling due to decentralized architecture

Future proof - Based on promise theory and many years of R&D

CFEngine 3.12 and beyond

- Security
- Testing, reliability and quality - CI
  - Deployment, scale, and reporting tests
  - Code analysis
  - Utilize modern technologies in continuous testing (Travis, Jenkins, codecov, LGTM, valgrind, ASAN)
  - Pull requests and releases are built and tested on 18 platforms
- Enterprise
  - Reporting
  - Usability
  - Mission Portal

cf-net

- A command line interface (CLI) to the CFEngine network protocol
- Introduced in CFEngine 3.10
- Uses the same code as cf-agent for network operations
  - Behaves like cf-agent (good for testing and reproducibility)
  - Open Source, written in C
  - Relies on command line arguments instead of policy
- Main use cases:
  - Debugging when an agent cannot fetch policy
  - Internal deployment, acceptance, and scale tests

Demo: cf-net

- Connect
  - Verify that host is online, server is listening and trust is established
- Stat
  - Check file type etc. of a policy file on the remote server
- Opendir
  - List contents of a directory
- Get
  - Download policy file from remote server, verify ACLs

Demo: cf-net help

CFEngine

```
$ cf-net help
Usage: cf-net [OPTIONS] command

Options:
  --help        , -h       - Print the help message
  --manpage     , -M       - Print the man page
  --host        , -H value - Server hostnames or IPs, comma-separated (defaults to policy server)
  --debug       , -d       - Enable debugging output
  --verbose     , -v       - Enable verbose output
  --log-level   , -g value - Specify how detailed logs should be. Possible values: 'error', 'warning',
'notice', 'info', 'verbose', 'debug'
  --inform      , -I       - Enable basic information output

Commands:
  help         - Prints general help or per topic.
                 Usage: cf-net help [command]
  connect      - Checks if host(s) is available by connecting.
                 Usage: cf-net -H 192.168.50.50,192.168.50.51 connect
  stat         - Look at type of file.
                 Usage: cf-net stat masterfiles/update.cf
  get          - Get file from server.
                 Usage: cf-net get masterfiles/update.cf -o download.cf [-jNTHREADS]
                        (%d can be used in both the remote and output file paths when '-j' is used)
  opendir      - List files and folders in a directory.
                 Usage: cf-net opendir masterfiles

Website: http://www.cfengine.com
This software is Copyright (C) 2008,2010-present Northern.tech AS.
$
```

Demo: cf-net connect

CFEngine

```
$ cat /var/cfengine/policy_server.dat
172.31.41.48
$ cf-net connect
Connected & authenticated successfully to '172.31.41.48'
$ cf-net -H localhost connect
Connected & authenticated successfully to 'localhost'
$
```

Demo: cf-net stat

CFEngine

```
$ cf-net stat /var/cfengine/masterfiles/
172.31.41.48:'/var/cfengine/masterfiles/' is a directory
$ cf-net opendir /var/cfengine/masterfiles/
cf_promises_validated
inventory
lib
promises.cf
cf_promises_release_id
templates
..
services
standalone_self_upgrade.cf
def.json
cfe_internal
.
update.cf
controls
$ cf-net opendir /var/cfengine/inputs/
$ cf-net stat /var/cfengine/inputs/
Could not stat: '/var/cfengine/inputs/'
$
```

Demo: cf-net get

CFEngine

```
$ ls
$ cf-net get /var/cfengine/masterfiles/promises.cf
$ ls
promises.cf
$ head promises.cf
#######################################################################
#
#   promises.cf - Basic Policy for CFEngine
#
#######################################################################

body common control
# @brief Control options common to all agents
{

$ echo "Test" > /var/cfengine/masterfiles/test.cf
$ cf-net get /var/cfengine/masterfiles/test.cf
$ head test.cf
Test
$
```

cf-remote

- Remotely deploy, install, upgrade, and bootstrap CFEngine in an automated fashion
- Python + fabric (SSH) tool
  - Open Source, in cfengine/core/contrib
  - Few dependencies:
    - Local: Python 3, Fabric, Requests, scp, curl
    - Remote: SSH, sh (cat, ls, which, cp, dpkg/rpm)
- Example use cases:
  - Installing and bootstrapping many hosts with a single command
  - Checking what CFEngine version is installed and whether it is bootstrapped

cf-remote - Demo

- Info
  - Log into a host, see information about OS and CFEngine version
- Packages
  - Find and download appropriate packages for given release + platform/OS
- Install
  - Transfer packages to remote machine, run installer, bootstrap
  - --demo for testing (Adds agent run, def.json, default credentials etc.)

Demo: cf-remote info

CFEngine

```
$ cf-remote info -H 18.203.139.187

ubuntu@18.203.139.187
OS           : ubuntu (debian)
Architecture : x86_64
CFEngine     : Not installed
Binaries     : dpkg, apt

$
```

Demo: cf-remote info (details)

CFEngine

```
$ cf-remote info -H 18.203.139.187 --log-level debug
[INFO] Set the log level to DEBUG
[DEBUG] Connecting to '18.203.139.187'
[DEBUG] Getting info about '18.203.139.187'
[DEBUG] Running over SSH: 'whoami'
[DEBUG] 'whoami' -> 'ubuntu'
[DEBUG] Running over SSH: 'uname'
[DEBUG] 'uname' -> 'Linux'
[DEBUG] Running over SSH: 'uname -m'
[DEBUG] 'uname -m' -> 'x86_64'
[DEBUG] Running over SSH: 'cat /etc/os-release'
[DEBUG] 'cat /etc/os-release' -> 'NAME="Ubuntu"
VERSION="18.04.1 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.1 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic'
[DEBUG] Running over SSH: 'which cf-agent'
[DEBUG] Running over SSH: 'cat /var/cfengine/policy_server.dat'
[DEBUG] Running over SSH: 'cf-agent --version'
[DEBUG] Running over SSH: 'which dpkg'
[DEBUG] 'which dpkg' -> '/usr/bin/dpkg'
[DEBUG] Running over SSH: 'which rpm'
```

Demo: cf-remote packages

CFEngine

```
$ cf-remote packages hub deb
Available releases: 3.13.0, 3.12.1, 3.12.0, 3.10.5, 3.10.4, 3.10.3, 3.10.2, 3.10.1, 3.10.0
Using 3.12.1 LTS (default):
Downloading package: '/Users/olehermanse/.cfengine/cf-remote/packages/cfengine-nova-hub_3.12.1-1_amd64.deb'
$ cf-remote --version 3.12.1 packages hub
Available releases: 3.13.0, 3.12.1, 3.12.0, 3.10.5, 3.10.4, 3.10.3, 3.10.2, 3.10.1, 3.10.0
Using 3.12.1 LTS:
Downloading package: '/Users/olehermanse/.cfengine/cf-remote/packages/cfengine-nova-hub-3.12.1-1.x86_64.rpm'
Package already downloaded: '/Users/olehermanse/.cfengine/cf-remote/packages/cfengine-nova-hub_3.12.1-1_amd64.deb'
$
```

Demo: cf-remote install

CFEngine

```
$ cf-remote install --hub 18.203.139.187 --version 3.12.1 --bootstrap 172.31.40.251 --demo

ubuntu@18.203.139.187
OS           : ubuntu (debian)
Architecture : x86_64
CFEngine     : Not installed
Binaries     : dpkg, apt

Package already downloaded: '/Users/olehermanse/.cfengine/cf-remote/packages/cfengine-nova-hub_3.12.1-1_amd64.deb'
Copying: '/Users/olehermanse/.cfengine/cf-remote/packages/cfengine-nova-hub_3.12.1-1_amd64.deb' to '18.203.139.187'
Installing: 'cfengine-nova-hub_3.12.1-1_amd64.deb' on '18.203.139.187'
CFEngine 3.12.1 was successfully installed on '18.203.139.187'
Bootstrapping: '18.203.139.187' -> '172.31.40.251'
Bootstrap succesful: '18.203.139.187' -> '172.31.40.251'
Transferring def.json to hub: '18.203.139.187'
Triggering an agent run on: '18.203.139.187'
Disabling password change on hub: '18.203.139.187'
Triggering an agent run on: '18.203.139.187'
Your demo hub is ready: https://18.203.139.187/ (Username: admin, Password: password)
$
```

cf-remote - Vote on syntax for file input

CFEngine

A. “Normal” path prefixes (~ ./ ../ /)
   a. cf-remote install --clients ./clients.txt
   b. cf-remote install --clients ../clients.txt
   c. cf-remote install --clients ~/clients.txt
   d. cf-remote install --clients /clients.txt
   e. ~~cf-remote install --clients clients.txt~~

B. @-prefix
   a. cf-remote install --clients @./clients.txt
   b. cf-remote install --clients @../clients.txt
   c. cf-remote install --clients @~/clients.txt
   d. cf-remote install --clients @/clients.txt
   e. cf-remote install --clients @clients.txt

cf-check - Background

- CFEngine uses local databases to communicate information between binaries and executions
  - “Last seen” hosts
  - Persistent classes
  - Promise locks
- Lightning Memory-Mapped database (LMDB) is the preferred database backend
  - Issues with corrupt / large databases on some platforms
  - Deleting database files generally fix these issues
- Before evaluating policy, agent has to open databases
  - Detecting corrupt databases in policy is a chicken and egg problem

cf-check

- Diagnose and fix corrupt local databases in CFEngine installations
- Written in C, initially based on lmdump tool
  - Open Source, available in cfengine/core repository
  - Repair code has been incorporated into cf-execd and cf-agent, and can be enabled with an optional argument

cf-check - Details

CFEngine

```
297 ¬
298 static int fork_and_diagnose(const char *path)¬
299 {¬
300 ····const pid_t child_pid = fork();¬
301 ····if (child_pid == 0)¬
302 ····{¬
303 ········// Child¬
304 ········exit(diagnose(path));¬
305 ····}¬
306 ····else¬
307 ····{¬
308 ········// Parent¬
309 ········int status;¬
310 ········pid_t pid = waitpid(child_pid, &status, 0);¬
311 ········if (pid != child_pid)¬
312 ········{¬
313 ············return CF_CHECK_PID_ERROR;¬
314 ········}¬
315 ········if (WIFEXITED(status) && WEXITSTATUS(status) != CF_CHECK_OK)¬
316 ········{¬
317 ············return lmdump_errno_to_code(WEXITSTATUS(status));¬
318 ········}¬
319 ········if (WIFSIGNALED(status))¬
320 ········{¬
321 ············return signal_to_code(WTERMSIG(status));¬
322 ········}¬
323 ····}¬
324 ····return CF_CHECK_OK;¬
325 }¬
326 ¬
```

Demo: cf-check

- Dump
  - Iterate through and print contents of a database file
- Diagnose
  - Fork processes, open and dump databases, check for errors
- Remove
  - Delete databases classified as corrupt
- Repair
  - Diagnosis and remove in one command

Demo: cf-check help

CFEngine

```
$ cf-check help

cf-check:
        Utility for diagnosis and repair of local CFEngine databases.
        This BETA version of the tool is for testing purposes only.

Commands:
        dump - Print the contents of a database file
        diagnose - Assess the health of one or more database files
        backup - Copy database files to a timestamped folder
        repair - Diagnose, then backup and delete any corrupt databases
        version - Print version information
        help - Print this help menu

Usage:
        $ cf-check command [options]

Examples:
        $ cf-check dump -a /var/cfengine/state/cf_lastseen.lmdb
        $ cf-check diagnose
        $ cf-check repair

$
```

Demo: cf-check dump

CFEngine

```
$ cf-check dump -a /var/cfengine/state/cf_lastseen.lmdb
key: 0x7f13367f3ed8[14] a172.31.39.43, data: 0x7f13367f3ee6[69] SHA=05b8f153c84e54a8d382ae36578adf2c2e2ad11027ea09678993e49003783e0c
key: 0x7f13367f3f34[70] kSHA=05b8f153c84e54a8d382ae36578adf2c2e2ad11027ea09678993e49003783e0c, data: 0x7f13367f3f7a[13] 172.31.39.43
key: 0x7f13367f3e60[71] qiSHA=05b8f153c84e54a8d382ae36578adf2c2e2ad11027ea09678993e49003783e0c, data: 0x7f13367f3ea7[40] ?QG\
key: 0x7f13367f3f90[71] qoSHA=05b8f153c84e54a8d382ae36578adf2c2e2ad11027ea09678993e49003783e0c, data: 0x7f13367f3fd7[40] ?QG\
$
```

Demo: cf-check diagnose

CFEngine

```
$ cf-check diagnose
    info: No filenames specified, defaulting to .lmdb files in /var/cfengine/state/
    info: Status of '/var/cfengine/state/nova_track.lmdb': OK
    info: Status of '/var/cfengine/state/packages_installed_$(package_module_knowledge.platform_default).lmdb': OK
    info: Status of '/var/cfengine/state/cf_observations.lmdb': OK
    info: Status of '/var/cfengine/state/history.lmdb': OK
    info: Status of '/var/cfengine/state/cf_changes.lmdb': OK
    info: Status of '/var/cfengine/state/nova_measures.lmdb': OK
    info: Status of '/var/cfengine/state/packages_updates_apt_get.lmdb': OK
    info: Status of '/var/cfengine/state/nova_static.lmdb': OK
    info: Status of '/var/cfengine/state/cf_lock.lmdb': OK
    info: Status of '/var/cfengine/state/cf_lastseen.lmdb': OK
    info: Status of '/var/cfengine/state/cf_state.lmdb': OK
    info: Status of '/var/cfengine/state/performance.lmdb': OK
    info: Status of '/var/cfengine/state/nova_agent_execution.lmdb': OK
    info: Status of '/var/cfengine/state/packages_installed_apt_get.lmdb': OK
    info: All 14 databases healthy
$
```

Demo: cf-check repair

CFEngine

```
$ echo "ConfigManagementCamp2019 - cf-check" > /var/cfengine/state/cf_lastseen.lmdb
$ cf-check repair
    info: No filenames specified, defaulting to .lmdb files in /var/cfengine/state/
    info: Status of '/var/cfengine/state/nova_track.lmdb': OK
    info: Status of '/var/cfengine/state/packages_installed_$(package_module_knowledge.platform_default).lmdb': OK
    info: Status of '/var/cfengine/state/cf_observations.lmdb': OK
    info: Status of '/var/cfengine/state/history.lmdb': OK
    info: Status of '/var/cfengine/state/cf_changes.lmdb': OK
    info: Status of '/var/cfengine/state/nova_measures.lmdb': OK
    info: Status of '/var/cfengine/state/packages_updates_apt_get.lmdb': OK
    info: Status of '/var/cfengine/state/nova_static.lmdb': OK
    info: Status of '/var/cfengine/state/cf_lock.lmdb': OK
    info: Status of '/var/cfengine/state/cf_lastseen.lmdb': SYSTEM_ERROR 183 - Unknown
    info: Status of '/var/cfengine/state/cf_state.lmdb': OK
    info: Status of '/var/cfengine/state/performance.lmdb': OK
    info: Status of '/var/cfengine/state/nova_agent_execution.lmdb': OK
    info: Status of '/var/cfengine/state/packages_installed_apt_get.lmdb': OK
   error: Problems detected in 1/14 databases
  notice: 1 corrupt database to fix
    info: Backing up to '/var/cfengine/backup/1548178159/'
    info: Copying: '/var/cfengine/state/nova_track.lmdb' -> '/var/cfengine/backup/1548178159/nova_track.lmdb'
    info: Copying: '/var/cfengine/state/packages_installed_$(package_module_knowledge.platform_default).lmdb' -> '/var/cfengine/backup/1548178159/
packages_installed_$(package_module_knowledge.platform_default).lmdb'
    info: Copying: '/var/cfengine/state/cf_observations.lmdb' -> '/var/cfengine/backup/1548178159/cf_observations.lmdb'
    info: Copying: '/var/cfengine/state/history.lmdb' -> '/var/cfengine/backup/1548178159/history.lmdb'
    info: Copying: '/var/cfengine/state/cf_changes.lmdb' -> '/var/cfengine/backup/1548178159/cf_changes.lmdb'
    info: Copying: '/var/cfengine/state/nova_measures.lmdb' -> '/var/cfengine/backup/1548178159/nova_measures.lmdb'
    info: Copying: '/var/cfengine/state/packages_updates_apt_get.lmdb' -> '/var/cfengine/backup/1548178159/packages_updates_apt_get.lmdb'
    info: Copying: '/var/cfengine/state/nova_static.lmdb' -> '/var/cfengine/backup/1548178159/nova_static.lmdb'
    info: Copying: '/var/cfengine/state/cf_lock.lmdb' -> '/var/cfengine/backup/1548178159/cf_lock.lmdb'
    info: Copying: '/var/cfengine/state/cf_lastseen.lmdb' -> '/var/cfengine/backup/1548178159/cf_lastseen.lmdb'
    info: Copying: '/var/cfengine/state/cf_state.lmdb' -> '/var/cfengine/backup/1548178159/cf_state.lmdb'
    info: Copying: '/var/cfengine/state/performance.lmdb' -> '/var/cfengine/backup/1548178159/performance.lmdb'
    info: Copying: '/var/cfengine/state/nova_agent_execution.lmdb' -> '/var/cfengine/backup/1548178159/nova_agent_execution.lmdb'
    info: Copying: '/var/cfengine/state/packages_installed_apt_get.lmdb' -> '/var/cfengine/backup/1548178159/packages_installed_apt_get.lmdb'
    info: Removing: '/var/cfengine/state/cf_lastseen.lmdb'
  notice: Database repair successful
$
```

cf-policy-upgrade

- Help users upgrade their policy to the latest version
- Scan /var/cfengine/masterfiles to find which files have manual edits and what can be automatically upgraded
- Python tool, doesn’t require git/version control

cf-policy-upgrade - Examples

CFEngine

```
fd1cf7a4cd7491a005d92a185dba2cc94d9e7e89fabba0233224061ab9518682 ./cfe_internal/CFE_cfengine.cf
a023bf9efeaf92fcec450cb13b0270b16902c9b0d3e6098b98273f6d61ff94d1 ./cfe_internal/core/deprecated/cfengine_processes.cf
1d6c806d1052f08bba7c053e97e5ba43dc0f9ce39765b13abb9659089d02d794 ./cfe_internal/core/host_info_report.cf
696d24ade7d360f3ed7596686daa556bcc8359e5ef12ecdfe3183895c898237e ./cfe_internal/core/limit_robot_agents.cf
4fe861ec8cc5b2954fa3626cc5e8961e467fd9a23df60026a491875a5fc0e5e0 ./cfe_internal/core/log_rotation.cf
2db6c4e6741b43d543ef166e92fb525f144793fff46bd896a939943790b4bb87 ./cfe_internal/core/main.cf
34f49e759800bcbc1d8ea9e8438646a406f46f1d035d8a6e7912eb76b7c6c663 ./cfe_internal/enterprise/CFE_hub_specific.cf
7c15513a511961ced9917b7270d9a4acf955ab587e0dfa6908bda2c534f1bab8 ./cfe_internal/enterprise/CFE_knowledge.cf
ad3b2cd4b1ee05428e740d8df8561b9b4f4551c8da2cf5c7a93c0a86222a4f43 ./cfe_internal/enterprise/file_change.cf
4e5df8287fa1ba3a67d2947a1f906275ac8a2320a66528341d98d15021178817 ./cfe_internal/enterprise/ha/ha.cf
487427eb98feb69a725f8617eb8f6580dd73c3aca05d4ae59ac381f37e96b346 ./cfe_internal/enterprise/ha/ha_def.cf
8ae274fcb3037817390aaec854d79f8f1811402fb3bb720d3ffc2c02124087c7 ./cfe_internal/enterprise/ha/ha_info.json
8b1edb6a441e9b7dc3b1efa7de31047625d9563d2648a62dca2fbe2d6564d25e ./cfe_internal/enterprise/ha/ha_update.cf
125a33bd27bfcee1a25fc7387fca52be3046755c9348633123f0585d5a6a588d ./cfe_internal/enterprise/main.cf
ac90dc71d6a6938acbc426679dd2963e04ea8f3a4655d7c6f83a7c6936f7cad1 ./cfe_internal/update/cfe_internal_dc_workflow.cf
a9302a5bb2ba7c93f4e6a20eb3b11a634f7618752cc1d11addaee243f0865c33 ./cfe_internal/update/cfe_internal_local_git_remote.cf
b8dd3d1d75f93e16b43b9056088f71bc19201b809dda8f6da033e2d2cbfe252e ./cfe_internal/update/cfe_internal_update_from_repository.cf
8459bdf07d5c78e4ea0c1d8a1f68085e87d03911fb09124472ee113a52fd0ac9 ./cfe_internal/update/update_bins.cf
eaba5d508f02929f621a7327db8693af5d732076506670aaf72ae0c7a609ffbc ./cfe_internal/update/update_policy.cf
fa5b6af43651e697c7202f8955949c16bbf72c27fdbee3464854d9d48b7e4365 ./cfe_internal/update/update_processes.cf
```

cf-policy-upgrade - Examples

CFEngine

```
"a98cc0df548411df5b59b26c4f12e6f3dd5c358bbe24efa1050b6f614fae3c26": [
  "3.7.6 ./promises.cf"
],
"./promises.cf": [
  "3.7.6 a98cc0df548411df5b59b26c4f12e6f3dd5c358bbe24efa1050b6f614fae3c26",
  "3.10.0 4f8ded74bbc1864228232b2a5c1c5ec968f2c81069774be8f0643db49f9c90a9",
  "3.10.1 e31f54f9f0760adb33170451e0d4556d826a9e437312871a120ab51304d692f6",
  "3.10.2 d973b288092d08e8eb09cc74263147dfeaf8df10bab109d5befa014341f8cdc2",
  "3.10.3 8209cc2e4e6f600a84ed74a884953f448cf091911a4c351ae32fd2b6a2516610",
  "3.12.0 a9de37c343a8e6b90409fa23f36ddc51d9c07779a30b141edc33019533cf8201",
  "3.12.1 9b306bde5aa886cb9855339fc6e67c6e80979c82728697f5bae692eed761371b"
],
```

cf-policy-upgrade - Examples

CFEngine

```
$ python3 ../masterfiles/contrib/policy_upgrade/scan_mpf.py
You are running version 3.12.1
$ echo "Custom policy" >> services/autorun/cfgmgmtcamp2019.cf
$ python3 ../masterfiles/contrib/policy_upgrade/scan_mpf.py
Custom policy: ./services/autorun/cfgmgmtcamp2019.cf
You are running version 3.12.1
$
```

cf-policy-upgrade - Examples

CFEngine

```
$ python3 ../masterfiles/contrib/policy_upgrade/scan_mpf.py
Renamed/copied policy: 3.12.1 ./controls/cf_agent.cf -> ./controls/agent.cf
This policy differs from masterfiles: ./controls/cf_execd.cf
This policy differs from masterfiles: ./controls/cf_serverd.cf
This policy differs from masterfiles: ./promises.cf
This policy differs from masterfiles: ./update.cf
You are running version 3.10.3
$
```

CFEngine

Questions?

Contribute code

- C
  - cf-net recursive copy
  - cf-check on windows (process spawning without fork)
  - cf-check data specific validation (example: check that timestamps are within reasonable range)
  - cf-check better database printing (look at mdb_dump for inspiration, and cf-key -s)
- Python
  - cf-remote package manager/platform support (yum, apt, installp, windows/msi)
  - cf-policy-upgrade interactive policy upgrade mode
  - cf-remote integration with AWS, Digital Ocean or Google Cloud. Automatically spawn desired VMs.

Contact

CFEngine

- CFEngine
  - cfengine.com
  - cfengine.com/blog
  - github.com/cfengine/core
  - github.com/cfengine/masterfiles
- Speaker
  - @olehermanse
  - ole@cfengine.com

CFEngine

Suggestions/Ideas?