CFEngine 3

Nástroj pro hromadnou správu

Úvod

- Marek Petko
  - Student KIV
  - ININ-DSP Distribuované systémy a počítačové sítě
- Hromadná správa výpočetních systémů v heterogenním prostředí
  - Diplomová práce pro CIV
  - Michal Švamberg (vedoucí práce)

Motivace

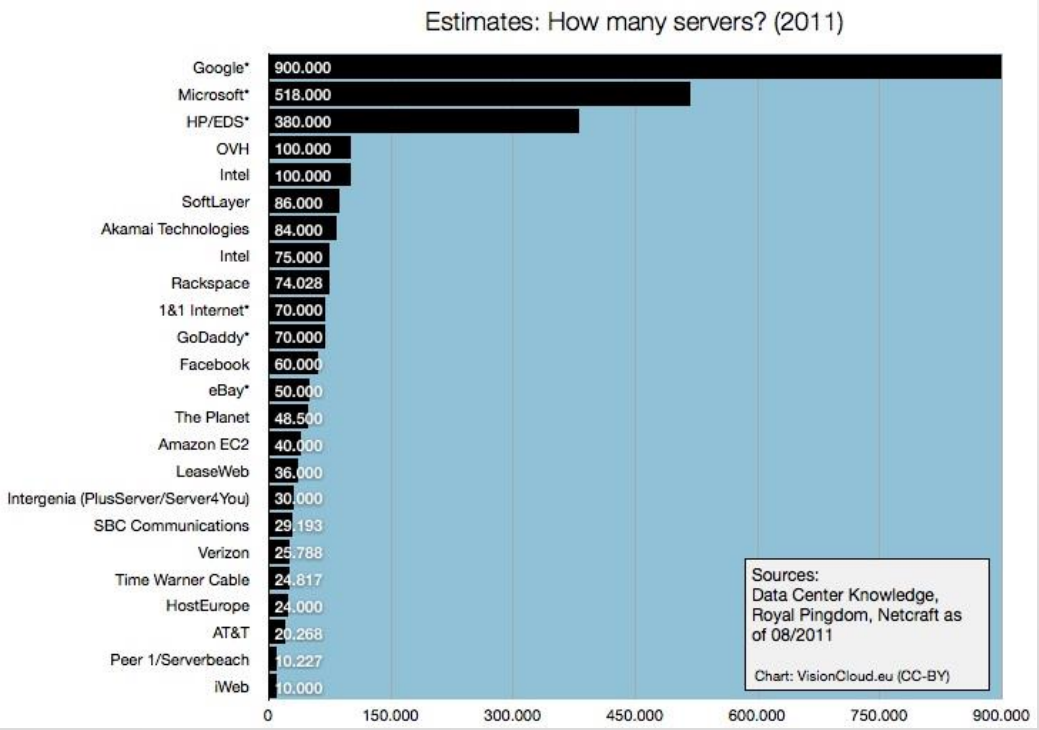
- Rozsáhlá datacentra
- Clustery
- Cloudy

Počet adminů

vs.

Počet serverů

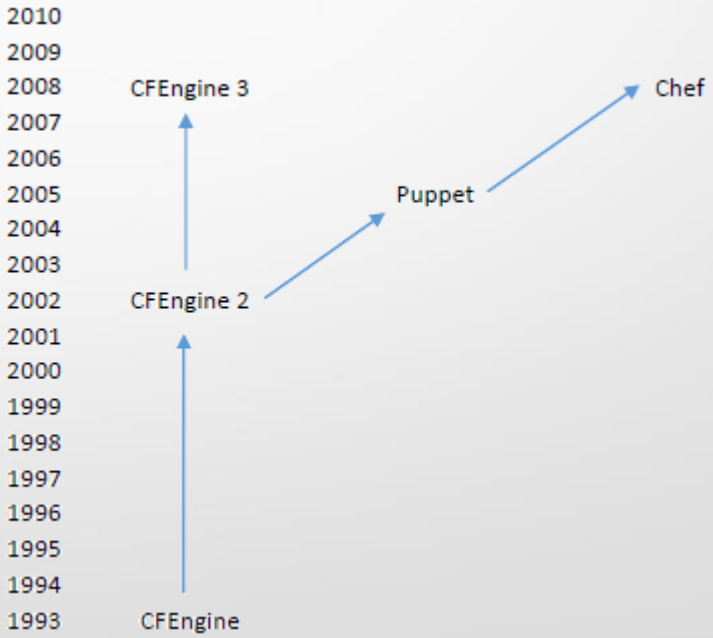
Přímá úměrnost?



Možnosti

- CFEngine
- Puppet
- Chef

- Open Source
- Enterprise



Placené verze

Servery	Počet	CFEngine 1 rok	CFEngine 3 roky	CFEngine 1 rok Education	CFEngine 3 roky Education	Puppet 1 rok	Chef 1 rok
GNU/Linux Debian	250	482 500 Kč	335 000 Kč	241 250 Kč	167 500 Kč	502 500 Kč	323 000 Kč
Windows Server	25	48 250 Kč	33 500 Kč	24 125 Kč	16 750 Kč	50 250 Kč	32 300 Kč
Oracle Solaris	11	21 230 Kč	14 740 Kč	10 615 Kč	7 370 Kč	22 110 Kč	14 212 Kč
VMWare ESXi	3	5 790 Kč	4 020 Kč	2 895 Kč	2 010 Kč	6 030 Kč	3 876 Kč
Celkem	289	557 770 Kč	387 260 Kč	278 885 Kč	193 630 Kč	580 890 Kč	373 388 Kč
1 uzel	1	1 930 Kč	1 340 Kč	965 Kč	670 Kč	2 010 Kč	1 292 Kč

CFEngine 3

- Silný teoretický základ
  - Teorie slibů (Mark Burgess)
- Vývoj
  - Důraz na efektivitu (Kompilované C)
  - Důraz na bezpečnost
- != CFEngine 2

Distribuce politiky

- Klient – server
  - Pouze pull
  - Možno force pull
  - Nikdy push (bezpečnost)
- Politika
  - Se zpracovává pouze lokálně, autonomně
  - Ze serveru se pouze kopíruje (ale nemusí!)
  - Na serveru plaintext – na klientech plaintext

Souborová struktura

/var/cfengine/

- **bin** – binární spustitelné soubory
- **inputs** – politika k lokálnímu spuštění cf-agentem
- **lastseen** – "Log data for incoming and outgoing connections."
- **lib** – knihovny (=! standardní knihovna)
- **masterfiles** – repositář politik na serveru
- **modules** – složka pro moduly
- **outputs** – výstupy cf-agenta (jen reports:)
- **ppkeys** – klíče
- **reports** – seznamy opravených promise (jen Enterprise)
- **share** – dokumentace, příklady, zdrojové kódy, atd.
- **state** – stavová databáze

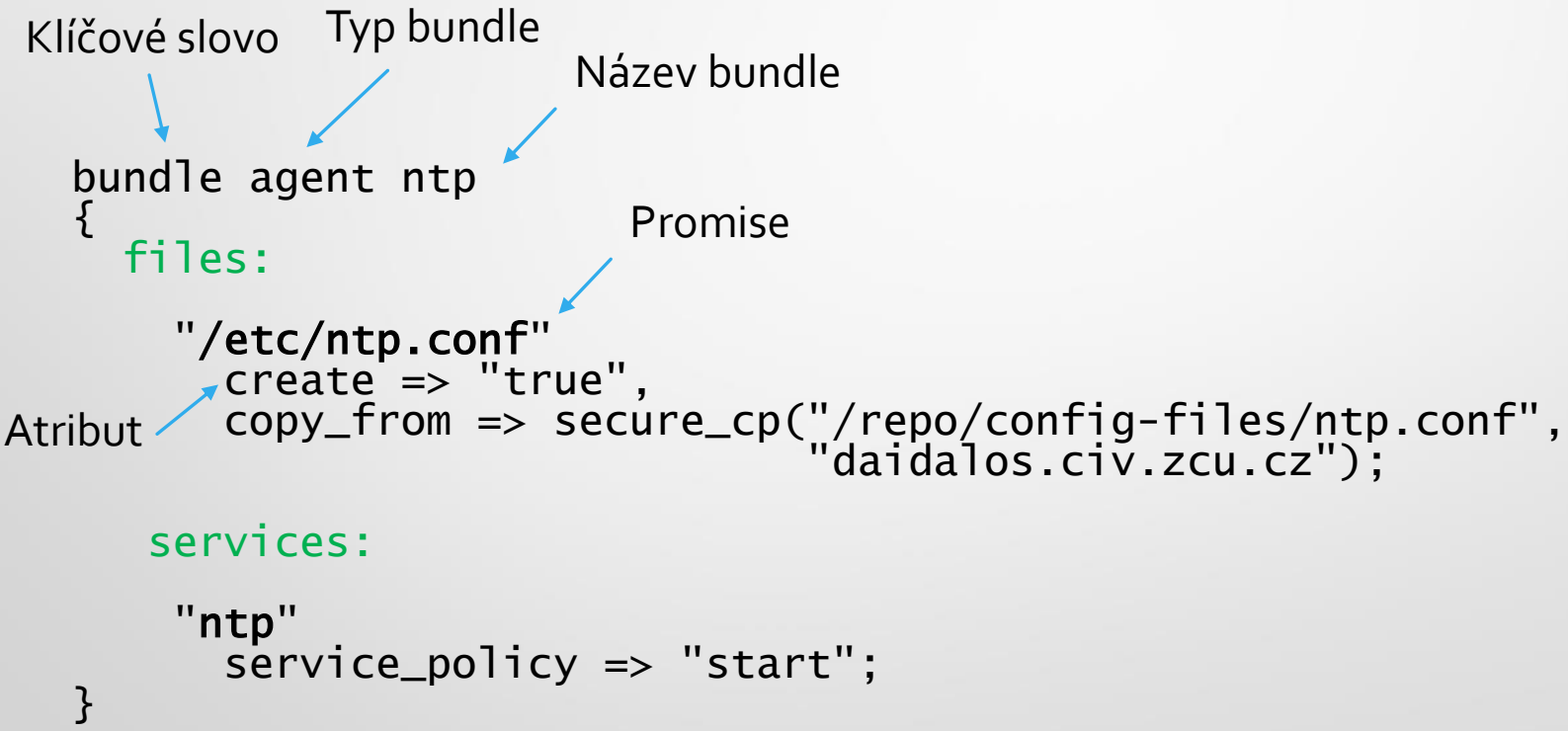
Koncepce jazyka

- Deklarativní jazyk
- Cokoliv je slib (promise)

Struktura

- Bundle ~ subrutina, procedura...
  - Promise type
    - Class
      - Promise

Ukázkový bundle




```
bundle agent ntp
{
  files:

    "/etc/ntp.conf"
      create => "true",
      copy_from => secure_cp("/repo/config-files/ntp.conf",
                             "daidalos.civ.zcu.cz");

  services:

    "ntp"
      service_policy => "start";
}
```

Typy promise

- **vars:** – Proměnné
- **classes:** – Třídy
- **files:** – Soubory
- **packages:** – Balíky
- **methods:** – Spouštění bundle
- **processes:** – Procesy
- **services:** – Služby
- **commands:** – Příkazy
- **reports:** – Výpis do konzole/e-mailu

Proměnné

```
bundle agent promenne
{
  vars:

    "retezec" string => "Retezec";
    "celociselna" int => "999";
    "realna" real => "1234.56";
}
```

Použití proměnné

- Lokálně: `$(promenna)`
- Globálně: `$(nazev_bundle.promenna)`

Seznamy

```
bundle agent seznamy
{
  vars:

    "retezce"
       slist => {"První", "Druhá", "Třetí"};

    "celociselne"
       ilist => {"1", "2", "3"};

    "realne"
       rlist => {"1.23", "4.56", "7.89"};
}
```

Asociativní pole

```
bundle agent asociativni_pole
{
  vars:

    "pole_uzivatelu[jgroll]„
       string => "Josef Groll";

    "pole_uzivatelu[aholecek]„
       string => "Antonín Holeček";

    "pole_uzivatelu[flesner]„
       string => "František Lešner";

  reports:

    "V městě Plzni působil $(pole_uzivatelu[jgroll])";
}
```

Implicitní iterace

```
bundle agent iterace
{
  vars:
    "maso"
      slist => {"vepřové", "kuřecí", "hovězí", "jehněčí"};

  reports:
    "Máma mele $(maso) maso.";
}
```

Třídy

```
bundle agent hard_class
{
  reports:

    linux::
      "Tento klient používá Linux!";

    solaris::
      "Tento klient používá Solaris!";

    windows::
      "Tento klient používá Windows!";
}
```

Body

- Sloučení atributů do znovupoužitelného celku
- Možnosti:
  - Uživatelské body – vlastní nastavení atributů
  - Předdefinované body – standardní knihovna
- Body lze jen „vyplnit“ (~implementovat interface)
- Nelze definovat vlastní strukturu

Ukázka body (1)

```
bundle agent example
{
  files:
    "/home/bill/id_rsa.pub"
      perms => system,
      create => "true";
}

body perms system
{
  mode => "644";
  owners => { "root" };
  groups => { "root" };
}
```

Ukázka body (2)

```
bundle agent example
{
  files:
    "/home/bill/id_rsa.pub"
      perms => mog("600", "bill", "sysop"),
      create => "true";
}

body perms mog(mode,user,group)
{
  owners => { "$(user)" };
  groups => { "$(group)" };
  mode   => "$(mode)";
}
```

Nasazení na CIVu

- CFEngine Community 3.5.2
- Server: **cf.civ.zcu.cz (daidalos.civ.zcu.cz)**
- 19 klientů
- Všechny nově instalované Debian servery přes FAI

Jak poznat CFEngine klienta (1)

- Klient běží

```
# ps ax | grep cf-

2036 ?        Ss    55:49 /var/cfengine/bin/cf-execd
2130 ?        Ss   321:49 /var/cfengine/bin/cf-serverd
2170 ?        Ss   105:38 /var/cfengine/bin/cf-monitord
28979 pts/0    S+     0:00 grep cf-
```

- Dočasné vypnutí

```
# /etc/init.d/cfengine3 stop
```

Jak poznat CFEngine klienta (2)

- Kolize s CFEnginem při editaci souboru
- Např. `/etc/apt/sources.list`

```
# CF3 - spravuje CFEngine3 - vsechny upravy budou zruseny
```

- Přístupy k editaci souborů
  - Celý zkopírovat
  - Template
  - Řádkové úpravy

Správa verzí politiky

- Udržování kompletní historie úprav
- Víceuživatelský přístup
- Vytváření vlastních větví konfigurace

↳ GIT na AFS

Větve konfigurace

- Master (devel)
- Production

- Přiřazení strojů v def.cf
  - Master – vyjmenovány
  - Production – vše ostatní

- Při aktualizaci politiky se stáhne příslušná větev

```
classes:
  "branch_master"
     or => {
      "cicomexocitl_civ_zcu_cz",
      "daphne_civ_zcu_cz",
      "metalist_civ_zcu_cz",
      "kiosek_tv10",
     };
```

Rozšíření změn

- Automaticky
- CFEngine na serveru spustí modul pro kontrolu GIT repositáře
  - Změna ve větvi → git pull
- cf-agent je spouštěn každých 5 min plošně
  - Po provedení změny až 5 min než se přesune z GITu na CF server
  - Dalších až 5 min než se přesune ze serveru na klienta
  - Nový klient až 15 minut!

Proces změn

`file:///afs/zcu.cz/project/software/git/cfengine.git`

1. Lokální klon repositáře
2. Nová lokální větev
3. Úpravy a testování na lokálním PC
4. Merge a push do testovací větve v repositáři
5. Kontrola na testovacích strojích
6. Merge a push do produkční větve

Podrobně: http://support.zcu.cz/index.php/LPS:CFEngine3

Struktura politiky

- **controls/** – konfigurace komponent
- **files/** – soubory ke kopírování na klienty
- **inventory/** – průzkum systému a vytváření nových tříd
- **lib/** – standardní knihovna
- **modules/** – moduly
- **services/** – vlastní politiky podle service oriented přístupu
- **templates/** – templaty ke kopírování na klienty
- **tests/** – pokusy
- **zcuinventory/** – průzkum systému a vytváření nových tříd
- **zculib/** – vlastní knihovna
- **def.cf** – nastavení proměnných pro konfiguraci
- **hosts.cf** – spouštění service bundlů podle hostů nebo skupin
- **promises.cf** – vstupní bod politiky
- **update.cf** – proces aktualizace politik na klientech ☠ ☠ ☠

Reporty

- V Enterprise verzi se zpětná vazba ukládá do centrální DB na serveru
- V Community verzi neexistuje zpětná vazba (záměrně)
- Řešení třetích stran pro sběr dat nejsou
- Reporty o anomáliích musí být vytvořeny ručně
  - Používá se promise typu reports:
  - Odesílá každý klient e-mailem Listovi
  - Použití více adres je možné jen změnou kódu politiky (konfigurace)

Bezpečnost (1)

2.2 The principles of CFEngine security

CFEngine adheres to the following design principles:

1. It shall be, by design, impossible to send policy-altering data to a CFEngine agent. Each host shall retain its right to veto policy suggestions at all times. This is called the **Voluntary Cooperation Model**.
2. CFEngine will support the encryption of data transmitted over the network.
3. Each host shall continue to function, as far as possible, without the need for communication with other hosts.
4. CFEngine will use a lightweight peer model for key trust (like the Secure Shell). No centralized certficate authority shall be used. SSL and TLS shall not be used.
5. CFEngine shall always provide safe defaults, that grant no access to other hosts.

http://cfengine.com/manuals_files/SpecialTopic_Security.pdf

Bezpečnost (2)

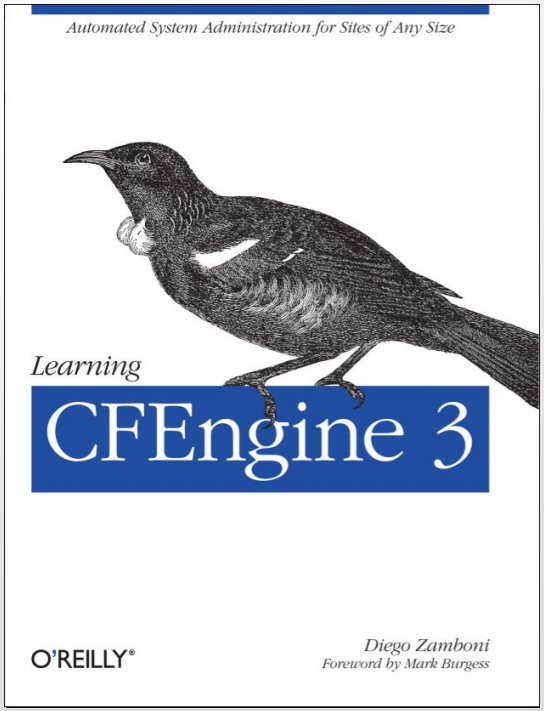
- Omezení klientů per IP
  - allowconnects, denyconnects
- Community
  - Autentizace – RSA 2048 public key
  - Šifrování – Blowfish 128
  - Challenge response – MD5 hash
- Enterprise
  - Autentizace – RSA 2048 public key
  - Šifrování – AES 256
  - Challenge response – SHA 256

Placená verze

- Sběr zpětné vazby do centrální DB
- Reporting
- Mission Portal
- Design Center GUI
- Windows nativně (instalace msi, registry, LDAP)
- Solaris

Dokumentace

- Manuály, reference, příklady
  https://cfengine.com/docs/3.5/
- Někdy přehlednější
  https://cfengine.com/archive/manuals/
- Kniha
  http://shop.oreilly.com/product/0636920022022.do
- Diskusní skupina
  https://groups.google.com/forum/#!forum/help-cfengine
- Bugtracker
  https://cfengine.com/dev/projects/core



Závěr

- CFEngine je velmi silný nástroj s budoucností
- Naučit se psát politiky chce trochu cviku
- V Community verzi chybí reporting ☹

Dotazy

Ukázka

```
#######################################################################
#
#   update.cf - Basic Update Policy for Community
#
#######################################################################

body common control
{
 bundlesequence => { "def", "cfe_internal_update" };
 version => "Community Update.cf 3.5.2";

 inputs => { "def.cf" };
}

#######################################################################

body agent control
{
 ifelapsed => "1";
 skipidentify => "true";
}

#######################################################################

bundle agent cfe_internal_update
{
 vars:
  any::

   "inputs_dir"         string => translatepath("$(sys.workdir)/inputs"),
                       comment => "Directory containing Cfengine policies",
                        handle => "update_vars_inputs_dir";


   "modules_dir"        string => translatepath("$(sys.workdir)/modules"),
                       comment => "Directory containing CFEngine modules",
                        handle => "update_vars_modules_dir";

   "ppkeys_file"        string => translatepath("$(sys.workdir)/ppkeys/localhost.pub"),
"repo/update.cf" 390L, 11838C                                                 1,1           Top
```