

3. 10. 2026



# Máte laC? A mohla bych ho vidět?

Štěpán Čmók



# Dobrá brazilská káva...



# Kdo jsem a o čem to bude...

- Štěpán Čmók
  - vedu tým Linuxářů ve Spořce
  - spravuju Linux 18 let - asi (vždy nějakou formou IaC)
- Infrastructure As (a) Code (IaC)
  - co to je?
  - k čemu to je?
  - proč to chtít?
  - je to pro mě?
  - doporučení
  - prostě předání poznatků a zkušeností...
  - ... a i malého příběhu
- Diskuze, otázky (ideálně na konec)



# Co tak běžně linuxáři řeší?

- **Milion věcí!!!** (jasně, záleží na rozdělení kompetencí a rolí ve Vaší firmě - různé úrovně zanoření linuxáka. My jsme celkem zanoření. Někde dělají čistě OS a dávají roota, a tak porůznu...)
  - Správa OS s celým životním cyklem (upgrady OS, patching, vulnerability, hardening, ...)
  - Clusterwary (třeba Pacemaker) + správa periférii jako SAN disků atd (btw. u nás **není** součástí IaC)
  - DNS zóny
  - Kerbeří realmy (vydávání keytabů a věcí s tím spojených, security, hardening, šifry, ...)
  - Webservery, případně celé farmy
  - Incidenty, change, problémy...
  - **Příprava podhoubí pro aplikace či platformy** (DB, aplikační servery, big data, ...)
    - § Každá appka jiné potřeby... Standardy řeší platformy (DB, Apl. servery, ...)
      - U nás "musí" Linux obsloužit vše (kde jaký krabicák a zhůvěřilost různého typu)
  - **Obecně - resources**
    - § Správa SW (repository, balíčky, verze, (latest) ...)
    - § Services (renderování unit, stavy: started, stopped, enable, disable, ... target (RL), ...)
    - § User management (uživatelé, skupiny, členství, ...)
    - § Renderování/templatování souborů, včetně konfiguračních....
    - § FS management (disky, fs, lv, vg, složky, mountování, credentials, nfs, cifs, ...)
    - § Elevace oprávnění (sudo, polkit ...)
    - § ...
  - Prostě co na očích našich zákazníků vidíme, ale... (k tomu se ještě dostaneme)
    - § → **musíme být připraveni prakticky na všechno!** → nezavírat si vrátka

# Dá se to dělat "ručně" (bez IaC)?

- Do určité velikosti prostředí **asi jo**.
  - ale přicházím i v malém prostředí o výhody IaC (dále)
- **Ruční správa**
  - Jít na server, nasekat příkazy, editovat soubory, ...
    - § Možná ssh cykly, skripty, playbooky, případně jiné nástroje (jednorázově)...
- v podstatě ale furt ručně
  - A jak víme...

**...ruční práce, to je dřina.**



# Hromadná správa a IaC



- Co to je IaC (někdy taky IaC nebo Config. Management.) ?
  - **Deklarativní popis stavu → Idempotence**
    - § Minimalizuje lidskou chybu (jasně, to známe)
  - Konfigurace se drží v gitu
    - § Change management, auditní stopa, "rychlý" návrat (podle charakteru změny)...
  - § **Otisk na servery v pravidelných intervalech! (obrázek soutěž?) → → → → →** 
    - Narovnávání stavu ručních zásahů i jiných, **obnovy serverů, upgrady (přesuny konfigurací mezi verzemi OS) !!!**
- **Standardizace! (jde to i bez ní, ale...) viz dále. (IaC dělá standardizaci nebo standardizace dělá IaC?)**
  - ... cesty, názvosloví, uživatelé, skupiny, fs, **standards**, ...
  - Každý "**špek**" (odklon od standardu) zvyšuje náročnost na správu. Linux umí "vše", ale někdy nechceme...
- **Spravujeme skupiny (krabičky) na rozdíl od jednotlivých serverů!!**
  - **Princip musí znát i zadavatelé!!!**
    - § rozvrhnout skupiny a dodržovat.
- **Hygiena práce**
  - Ne vždy se zdá, že to je výhodné.
    - § Konfigurák upravím za pár vteřin vs. pull úpravy v gitu, commit, pust, nasazení (když vím jak :-))
    - § V IaC musí být všechno (**co jsme si řekli! viz další strana**) → bolí to pak při upgradech, rozšiřování srv...)
    - § Je potřeba pro to **nakoupit lidi**. Když to někdo bude obcházet, je to na prd...
      - dává někdy smysl to obejít? příklady: jednorázovky, server před zrušením, ...

# A co že to tedy (ještě jednou) přináší?

- Verzování Vaší konfigurace
- Auditování Vaší konfigurace a činnosti s propsáním do Vašeho oblíbeného Change (Inc., prb, ...) managementu
  - dohledání změn, kdo, co, proč, kdy...
  - bacha na Commit messages!!! → zase je potřeba nějaký standard (zmínit číslo ticketu, ...)
- Dokumentace konfigurace a standardů prostředí
- Správa po skupinách
  - Nový server přidám do krabičky a je hotovo
    - **rychlost** (když už mám krabičku hotovou)
- Obnovy konfigurací (dr, rm -rf..., atd... )
  - někdy mohu vynechat zálohy (???!!! - **možná**)
- Konzistence
  - někdy víme my lépe než zákazníci, co chtějí... :-) (z jiných prostředí)
- ... Je to dost?

## V laC "vše, co jsme si řekli"

- je potřeba si udělat **nějakou čáru**, co do **laC** patří a co ne.
- Neznamená to (alespoň v našem podání), že je v laC všechno co je v OS
  - něco je součástí RPM, něco OS jako takového, někde jen řádky (line in file...)
- SAN disky, vgs, ... u nás mimo laC
- **Historie - příběh**
  - první "laC" - Satellite (tak nějak) - konfigurační soubory, rozložení fs, ...
  - pak nástup Puppet.

# Puppet 2 Ansible (Trocha toho příběhu...)

- Úplně původně Satellite (distribuce konfiguračních souborů, ...)
- Nutno řešit lifecycle puppet
- **Naše verze neměla agenty pro RHEL8+**
- Relativně drahé řešení.
- Nutno jednat!
  - § Přepis do nové verze Puppetu?
    - Celkový přepiš (nový puppet language atd...) Nešlo by jen o "rychlý" upgrade.
  - § Jiná technologie? Cf-engine, chef, ...
    - řešili jsme i otázku supportu, licencí, podpory, ...
    - Ansible
      - Zapadá do RedHat family (napojení na periferie (foreman, satellite → inventory) atd)
      - Ansible tu už tak jako tak byl/je → sjednocování technologií → zjednodušování
      - "zadarmo" (v rámci Redhat OS subskripce) → úspora blablabla
  - Poučení z historie
    - § Obecně **KISS** (Keep It Stupid Simple - povedlo se? :-)) - poučení z Puppet
    - § Roztržení týmů → Reorganizace git repozitářů
      - Každý si řeší svoji část oproti puppetu → připravenost na různé organizační změny, jasná odpovědnost
      - Repozitář pro sdílené objekty (viz dále)
  - **Migrace P2A - cca 5 let nazpět?**
    - § Za linux mega akce!
      - Co Tě nezabije, to Tě posílí. Tooly na migraci konfigurace z Puppet do Ansible. Vývoj inhouse
    - § Ale bohužel s ...

# ...kostlivci ve skříni



Přecijen ne vše bylo v  
gitu → vylámání zubů

# ACM - prostředí

- 
- ACM? - co že to je?
  - **Ansible Configuration Management** (made in Spořka) - **tak to děláme dnes**
- Environments (Git prostředí)
  - potřeba rozmyslet rollout a koncept. Sdílíme myšlenku i jinde.. (Satellite, ...)
  - Test – dev(a,b,c,d), int, prs, sys, edu, at(1,2,3), st(1,2,3), stage, qa ....
  - Pred - předprodukce
  - Prod - produkce
  - **Shared - sdílené objekty (proč? poučení z historie)**
    - Síťové mounty, useři, skupiny, (technické) ...
      - příklad s NFS
  - DTP perimetr - separovaný ostrůvek se vším (sítě atd,), nejen ACM
    - Dtp-nonprod – dataprotection nonprod
  - Dtp-prod – dataprotection prod
- Postupné nasazování přes prostředí
  - Separace
    - Konfigurací os/app
    - I samotných změn (devel) v ACM

# ACM – skupiny a hosti

- **Spravujeme po skupinách!**

- Host\_vars - konfigurace specifické pro hosta - server (nastavení sítě: ip adresa, mac/hw adresa, PBR, Hostname, ...)
  - výjimečně nějaká konfigurace do host\_vars.
    - přemýšlet co se vyplatí a být si vědom, že tam taky něco může být → práce v týmu
- Group\_vars – konfigurace pro skupinu
  - I jeden server má vlastní skupinu
  - Statické vs. Dynamické inventory
    - Statické v ACM nepoužíváme (./inventory/hosts) Jenom pro nějaké automatizátory
    - Vše dynamicky pomocí dynamic inventory (DI)
      - Spustitelné soubory v ./inventory/ (ukázka na další stránce)
        - **Inventory/foreman.py** - dodaný RedHatem napojený na Satellite (zdroj RH SW výbavy..)
          - Používaný k pravidelnému obrábění
          - **Cílová konfigurace serverů vznikne z kombinace tzv. HG a HC**
            - Host\_groups – server může být právě v jedné HG. Hlavní konfigurační směr.
            - Host\_collections – server může být v jedné a více HC. Pinovací charakter. Viz dále
        - **Inventory/linux.py** - vlastní výroba sosající data z vmware a CMDB (a jiných zdrojů)
    - Vše v cache, která se pravidelně refreshuje
      - výkon, rychlost, ... prostě cache

# ACM – ukázka env + DI

```
(A) :linux-acm-test$ ls ../../{acm,ntp} -l
```

```
../../acm:
```

```
linux-acm-pred  
linux-acm-prod  
linux-acm-shared  
linux-acm-test
```

```
../../ntp:
```

```
dataprotection-acm-prod  
dataprotection-acm-test
```

```
(A) :linux-acm-test$
```

```
(A) :linux-acm-test$ ll inventory/
```

```
total 188
```

|             |     |  |                    |                        |                                |
|-------------|-----|--|--------------------|------------------------|--------------------------------|
| lrwxrwxrwx. | 1   |  | 22 May 15 15:45    | foreman.ini ->         | ../secrets/foreman.ini         |
| lrwxrwxrwx. | 1   |  | 30 May 15 15:45    | foreman-preload.ini -> | ../secrets/foreman-preload.ini |
| -rwxr-x---  | 1   |  | 28076 May 15 15:45 | foreman.py             |                                |
| drwxr-x---  | 343 |  | 40960 Sep 10 11:04 | group_vars             |                                |
| -rw-r-----  | 1   |  | 21194 Sep 10 11:04 | hosts                  |                                |
| drwxr-x---  | 648 |  | 53248 Sep 10 11:04 | host_vars              |                                |
| lrwxrwxrwx. | 1   |  | 20 May 15 15:46    | linux.ini ->           | ../secrets/linux.ini           |
| lrwxrwxrwx. | 1   |  | 28 May 15 15:46    | linux-preload.ini ->   | ../secrets/linux-preload.ini   |
| -rwxr-x---  | 1   |  | 10381 May 15 15:46 | linux.py               |                                |
| -rw-r-----  | 1   |  | 490 Aug 2 07:41    | patchovka-hosts        |                                |
| -rw-r-----  | 1   |  | 987 May 15 15:46   | t.txt                  |                                |
| -rw-r-----  | 1   |  | 232 May 15 15:46   | vgs.txt                |                                |
| -rw-r-----  | 1   |  | 119 Jul 16 13:31   | xxx_hosts              |                                |

```
(A) :linux-acm-test$
```

# ACM – HG - názvosloví

**ELver/ENV/SERVER\_ROLE/{TECHNOLOGY,APPLICATION}/{GENERIC,CLUSTER,PROJECT,FARM,PURPOSE,...(odděleno podtržítka)}**

**el9\_test\_db\_oracle\_rac\_cluster01**

**el8\_pred\_as\_crm\_terminal**

- **HostGroup - udává hlavní konfigurační směr!!!**
  - **Vymyslete si systém!** zabere to čas. Investice do budoucna!
- Zanoření 5 úrovní
  - Možnost dědění konfigurace přes úrovně
    - hlavní je ale druhá (**ELver/ENV**) a poslední. Problémy s neustálým přepisováním dat. viz dále
- Poslední úroveň se dělí podtržítka a případně se obohacuje o další slova, technologie, potřeby, aplikace, kombinace ...
- Skupiny (HG) využíváme i jinde → **globální koncept**
  - Integrace na AD
    - Ale to zas třeba jindy... :-)
  - Obecná automatizace
    - Ad-hoc úkony
  - DR procedury
  - Viz dále

# ACM – HG - ukázka I.

| Name | OS                                                                                            | Owner                                                                                    | Host group           |
|------|-----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|----------------------|
|      |  RedHat 7.9  |  Adm... | el7/prod/ss/sas/...  |
|      |  RedHat 7.9  |  Tom... | el7/prod/ss/sas/...  |
|      |  RedHat 7.9  |  Adm... | el7/test/ss/sas/g... |
|      |  RedHat 8.10 |  Tom... | el8/test/ss/sas/...  |
|      |  RedHat 7.9  |  Adm... | el7/pred/ss/sas/...  |
|      |  RedHat 7.9  |  Tom... | el7/pred/ss/sas/...  |

```
foreman_host_group_el7_test_as_odi
foreman_host_group_el7_test_as_odm
foreman_host_group_el7_test_as_osb
foreman_host_group_el7_test_as_osb
```

[illegible]

s  
 sh  
 generic  
 generic  
 eric  
  
 lending\_int  
 lending\_sys  
  
 f  
  
 eric  
 final  
  
 generic  
 e  
  
 c  
 c\_amt  
 c\_arc  
 c\_backup  
 c\_cic  
 c\_col  
 c\_crm01  
 c\_detool  
 c\_edudb01

```
foreman_host_group_el8_test_is_og
foreman_host_group_el8_test_is_rt
foreman_host_group_el8_test_newse
foreman_host_group_el8_test_newse
foreman_host_group_el8_test_newse
foreman_host_group_el8_test_ss_ap
foreman_host_group_el8_test_ss_sa
foreman_host_group_el8_test_ss_sa
foreman_host_group_el8_test_ww_ar
foreman_host_group_el8_test_xx_cc
foreman_host_group_el8_test_xx_da
foreman_host_group_el8_test_xx_da
foreman_host_group_el8_test_xx_dm
foreman_host_group_el8_test_xx_dm
foreman_host_group_el8_test_xx_dm
foreman_host_group_el8_test_xx_dm
foreman_host_group_el8_test_xx_in
foreman_host_group_el8_test_xx_rt
foreman_host_group_el9_test
foreman_host_group_el9_test_ad_ap
foreman_host_group_el9_test_as_ar
foreman_host_group_el9_test_as_ce
foreman_host_group_el9_test_as_cm
foreman_host_group_el9_test_as_de
foreman_host_group_el9_test_as_el
foreman_host_group_el9_test_as_el
foreman_host_group_el9_test_as_pi
foreman_host_group_el9_test_as_po
foreman_host_group_el9_test_db_ap
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_db_or
foreman_host_group_el9_test_efi
foreman_host_group_el9_test_newse
foreman_host_group_el9_test_newse
foreman_host_group_el9_test_qs_ap
foreman_host_group_el9_test_ss_ap
foreman_host_group_el9_test_ww_ar
foreman_host_group_el9_test_xx_si
foreman_host_group_el9_test_xx_si
```

```

c
ric

m
assigned
_generic
c
_capsule
y_generic

tion_veritas_clients
tion_veritas_snapshotmanager

x

_dev
y_generic
ric

ols
c

_dev

ac
ac_dboradb02
ac_tboradb02

_tr03db

m
assigned
_dev
_dev
y_generic
k_as
k_is

```

# ACM – HG - ukázka II.

- Po automatické instalaci končí server v
  - foreman\_host\_group\_el<version>\_<env>\_newservers\_acm – viz prtscr
    - **Nutno dořešit konfiguraci a zařazení do finální HG!!!**
    - Na začátku lifecycle (nová apka, platforma), dáváme do
      - foreman\_host\_group\_el<version>\_<env>\_newservers\_unassigned
        - Kde se server obrábí **alespoň na úrovni OS**, bez app. Konfigurace. **Server nemůže ani bez appky zůstat neobráběný.**
          - Musí se aplikovat případné změny i na holý server/OS.
          - Někdy snad full automatizované doobrobení pro appku ...
            - **Tam je ale spousta výzev. A??? ...**

```
+++
#####
#
#   Server je nove nainstalovany.
#   Pro finalni konfiguraci je nutno server presunout do konecne hostgroupy a spustit ACM.
#
#####
+++
```

**...zase dřina!**



# ACM – HC

- **Host\_collection**
- Doplňuje hlavní konfigurační směr (HG)
  - Server může být v jedné a více HC
  - Pinovací charakter
  - Viz prtscr

```
foreman_hostcollection_el7_test_app agent_disabled
foreman_hostcollection_el7_test_cs
foreman_hostcollection_el7_test_gua
foreman_hostcollection_el7_test_imp
foreman_hostcollection_el7_test_ipx
foreman_hostcollection_el7_test_pac
foreman_hostcollection_el7_test_pod hexagrid
foreman_hostcollection_el7_test_sas
foreman_hostcollection_el7_test_sec opentest
foreman_hostcollection_el7_test_suc spectrum
foreman_hostcollection_el7_test_tsr
foreman_hostcollection_el7_test_tsr
foreman_hostcollection_el7_test_ver sclient_enabled
foreman_hostcollection_el7_test_ver sclient_lab_enabled
foreman_hostcollection_el8_test_app agent_disabled
foreman_hostcollection_el8_test_clo azure
foreman_hostcollection_el8_test_cs
foreman_hostcollection_el8_test_ipx
foreman_hostcollection_el8_test_sas
foreman_hostcollection_el8_test_tsr
foreman_hostcollection_el8_test_ver sclient_enabled
foreman_hostcollection_el8_test_ver sclient_lab_enabled
foreman_hostcollection_el9_test_el
foreman_hostcollection_el9_test_sas
foreman_hostcollection_el9_test_ver sclient_enabled
foreman_host_group_el7_test
```

# ACM – další možnosti skupin z DI

Nejen pro ACM, ale např. i Ad-HOC akce...

```
"ucmdb_cs_environment_pre_production",  
"ucmdb_cs_environment_production",  
"ucmdb_cs_environment_test",
```

```
"vmware_os_red_hat_enterprise_linux_6_32_bit",  
"vmware_os_red_hat_enterprise_linux_6_64_bit",  
"vmware_os_red_hat_enterprise_linux_7_64_bit",  
"vmware_os_red_hat_enterprise_linux_8_64_bit",  
"vmware_os_red_hat_enterprise_linux_9_64_bit",
```

```
"ucmdb_cs_maintenance_schedule_lin_pred_wave_db_2b_fri_14_00_18_00"  
"ucmdb_cs_maintenance_schedule_lin_pred_wave_db_2m_fri_10_00_14_00"  
"ucmdb_cs_maintenance_schedule_lin_pred_wave_qs_1_thu_09_00_13_00"  
"ucmdb_cs_maintenance_schedule_lin_prod_wave_as_10_dc2_sun_00_05_03_05"  
"ucmdb_cs_maintenance_schedule_lin_prod_wave_as_10m_dc2_sun_00_10_03_10"
```

```
"ucmdb_cs_loc_code_azure",  
"ucmdb_cs_loc_code_dc1",  
"ucmdb_cs_loc_code_dc2",  
"ucmdb_cs_loc_code_dc3",
```

```
"ucmdb_host_isvirtual_false", "vmware_srm_protection_group_pg_ ",  
"ucmdb_host_isvirtual_true", "vmware_srm_protection_group_pg_ ",  
"vmware_srm_protection_none",  
"vmware_srm_protection_srm_protected_synchronous_array_based_replication",
```

```
"vmware_host_name_  
"vmware_host_name_  
"vmware_host_name_  
"vmware_host_name_  
"vmware_host_name_
```

```
"ucmdb_discovered_model_poweredge_r740",  
"ucmdb_discovered_model_poweredge_r740xd",  
"ucmdb_discovered_model_poweredge_r750",  
"ucmdb_discovered_model_proliant_dl380_gen10",  
"ucmdb_discovered_model_proliant_dl380_gen10_plus",  
"ucmdb_discovered_model_proliant_dl380_gen11",  
"ucmdb_discovered_model_proliant_dl380_gen9",
```

## 2. Intermezzo

Kolik Linux OS máme u nás ve správě?

- a.) 0-500
- b.) 500-1000
- c.) 1000-3000
- d.) 3000-8000
- e.) více

# ACM – role/generická role

- Role dělají reálnou práci
- Redhat systémové role (každá jiná) vs. naše role.
  - ReHat role používáme třeba na výrobu pacemaker clusteru (byly potřeba úpravy, RH upravil...)
- Naše role
  - **Koncept generické role**
    - Jak jsem říkal, musíme být připraveni na vše...
    - **Každá role umí v základu vše!** (vše includované do ACM playbooku, viz dále)
      - Opět standardizace → každá role se obsluhuje stejně
        - Useři, balíčky, služby, soubory...
    - Dá se však obohatit, pokud je nutně potřeba
      - Např. Specifické instalace (udiscovery agent, snow agent), epa (viz dále), ad join, ...
  - **Oddělení kódu od dat**
    - zase poučení z historie (příběh)
    - Kód: ./playbooks/roles/
      - spouštění má své pořadí - nejdřív složka, pak fs, pak mount, atd.. (dá se měnit)
    - Data: ./inventory/group\_vars/<HG>
      - Koncept "krmítek" → všude stejná jména (krom jména role) - standard, koncept, ...
      - **Běžně lidi do kódu nesahají a plní jen krmítka daty**
        - Použitelné pro širší spectrum lidí, strmější učící křivka, ...

# ACM – kód (proč tolik rolí?)

```
(A) :linux-acm-test$ ls playbooks/roles/
csas_appdynagent  csas_elastic  csas_iptables  csas_networkmanager  csas_pgs  csas_sshd  csas_users  rhel-system-r
csas_audit        csas_epa      csas_ipx       csas_nfs              csas_postgres  csas_sssd  csas_veritasclient
csas_autofs       csas_guardium csas_krb5       csas_nftables        csas_processexporter  csas_sudo  csas_yum
csas_boot         csas_horcm   csas_krb5kdc   csas_nodeexporter    csas_rsyslog   csas_sysctl df_chrony
csas_cron         csas_ifcfg   csas_linux     csas_oracle          csas_sas       csas_tsm   df_ntp
csas_csops        csas_imperva csas_misc      csas_ovoagent        csas_security  csas_tuned df_postfix
csas_docker       csas_info    csas_named     csas_packages        csas_snowagent  csas_udagent generic_role

(A) :linux-acm-test$
(A) :linux-acm-test$ ls playbooks/roles/csas_boot/
defaults handlers meta tasks templates vars

(A) :linux-acm-test$
(A) :linux-acm-test$ ls playbooks/roles/csas_boot/tasks/RedHat8/
backup.yml empty.yml filesystems_fce_mounts_absent.yml pre_install.yml
config_fce_assemble_file.yml files_fce_acls_lists.yml filesystems_fce_mounts_present.yml services.yml
config_fce_copy_file.yml files_fce_acls.yml filesystems_fce_volume_groups_absent.yml uninstall.yml
config_fce_create_directory.yml files_fce_files_lists.yml filesystems_fce_volume_groups_present.yml users_fce_groups_local.yml
config_fce_create_file.yml files_fce_files.yml filesystems_fce_volumes_absent.yml users_fce_groups.yml
config_fce_insert_file.yml files_fce_nfs4acls_lists.yml filesystems_fce_volumes_present.yml users_fce_users_local.yml
config_fce_insert_line.yml files.yml filesystems.yml users_fce_users_remote.yml
config_fce_populate_directory.yml filesystems_fce_copy_file.yml install_fce_module.yml users_fce_users.yml
config.yml filesystems_fce_files_lists.yml install.yml users.yml
dump.yml filesystems_fce_files.yml post_install.yml

(A) :linux-acm-test$
(A) :linux-acm-test$ find playbooks/roles/csas_boot/templates/RedHat8/ | grep j2
playbooks/roles/csas_boot/templates/RedHat8/custom/foreman host_group_el8_test_db_oracle/etc/modprobe.d/lpfc.conf.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/default/grub.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/inittab.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/lvm/lvm.conf.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/modprobe.d/cis.conf.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/profile.d/runlevel.sh.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/rc.d/rc.local.j2
playbooks/roles/csas_boot/templates/RedHat8/default/etc/systemd/system/onboot.target.j2

(A) :linux-acm-test$
```

# ACM – data (krmítka) - YAML!!

```
(A) :linux-acm-test$ ls inventory/group_vars/foreman_host_group_el8_test/
appdynagent.yml  cron.yml        named.yml        ovoagent.yml     provider_firewall.yml  rsyslog.yml    sudo.yml        vault.yml
audit.yml        defaults.yml    networkmanager.yml  packages.yml     provider_mail.yml      security.yml    sysctl.yml      veritasclient.yml
boot.yml         info.yml        nfs.yml          postfix.yml      provider_network.yml   snowagent.yml  tsm.yml         yum.yml
chrony.yml       linux.yml       nftables.yml      provider_auth.yml provider_syslog.yml     sshd.yml       tuned.yml
cm.yml           misc.yml        nodeexporter.yml   provider_dns.yml provider_timesync.yml   sssd.yml       udagent.yml

(A) :linux-acm-test$
(A) :linux-acm-test$ head -n 24 inventory/group_vars/foreman_host_group_el8_test_is_away/epa.yml
---
role_csas_epa_epas:
- epa: 'tst_csops_aws'
  owner: '[REDACTED]'
  group: '[REDACTED]'
  app: {size: '1G', mode: '2755'}
  bin: {size: '1G', mode: '2755'}
  users:
    - {'name': '[REDACTED]', 'state': 'present', 'groups': [], 'append': yes}
  groups:
    - {'name': '[REDACTED]', 'state': 'present'}

- epa: 'tst_csops_csopsd'
  owner: 'root'
  group: 'root'
  app: { size: '1G', mode: '2755' }
  data: { size: '1G', mode: '2755' }
  log: { size: '5G', mode: '2755' }
  tmp: { size: '1G', mode: '1755', owner: '[REDACTED] group: '[REDACTED]

  packages:
    - { name: ['ncurses-libs.i686','zlib.i686','libgcc','nfs4-acl-tools','libstdc++.i686'], state: installed }
  epa_conf:
    - { dest: '/usr/local/bin/csopsd.sh', src: '{{ ansible_distribution }}{{ ansible_distribution_major_version }}/custom/tst_csops_csops
d/usr/local/bin/csopsd.sh.j2', owner: root, group: root, mode: '0755' }

(A) :linux-acm-test$
```

# ACM – vychytávky



# ACM – vychytávky

- Providers → Možnost výběru role

- Správa času

- Ntp vs. Chrony

- Firewall

- Iptables vs. nftables

- Atp...

- Csas\_epa

- Chytristika navíc oproti běžné roli (běžné resources + něco navíc)... viz ukázka krmítek 2 slides zpět

- **Dopočítávání → standardizace!!!** Opět - odklon od standardu, zvýšená pracnost

- Propojení se ServiceNOW

- Change do commit messages

- Hlavičky ansible managed

- S detaily, odkud se bere, ...

- Dumpování proměnných na serveru

- hodí se, např. k dohledávání...

- /var/tmp/acm/<role\_vars>\*

- /etc/acm-info

- Viz dále

```
(A) :foreman_host_group_el8_test$ ls *prov*
provider_auth.yml      provider_mail.yml      provider_timesync.yml
provider_dns.yml        provider_network.yml
provider_firewall.yml  provider_syslog.yml
(A) :foreman_host_group_el8_test$
(A) :foreman_host_group_el8_test$ cat *pro*fire*
---
role_provider_firewall: 'csas_nftables'
(A) :foreman_host_group_el8_test$
```



User [redacted] added a new commit: [redacted]cc4501c4 [redacted]  
epa: mounts t [redacted]dms\_07\_sma [redacted]rs, CHG [redacted]56

# ACM – /etc/acm-info. Info i pro jiné

```
(A) :~$ cat /etc/sinfo
# Ansible managed: /srv/data/prod/ansible/core/remote/cm/environments/test/playbooks/r
info

# Satellite:
NAME="
HOST_G
LOCATION="Prague/test"
ID="816"
SMART_PROXIES="

# uCMDB:
CS_ENVIRONMENT="Test"
CS_LOC_CODE="DC1"
CS_CI_OWNER="None"
CS_CLUSTER="None"
CS_FARM="None"
CS_ROLE="DB"
CS_SOFTWARE="None"
CS_PROJECT="INFRA"
CA_NAME="HSLV t
RESOURCE_CONTACT="None"
SUPPORT_CONTACT1_UUID="
DISCOVERED_OS_VENDOR="Red Hat"
HOST_OSINSTALLTYPE="Red Hat Enterprise Server"
DISCOVERED_OS_VERSION="7.9"
DISCOVERED_MODEL="Vmware Virtual Platform"
DISCOVERED_VENDOR="VMware, Inc."
HOST_ISVIRTUAL="True"
CS_IS_DMZ="false"
CS_HA_DR_TYPE="SRM protected (Synchronous Array-based Replication)"
CS_INSTALLER="None"
CS_MAINTAINER="None"

# VMware:
VM_NAME="
NOTES="29. července 2021 14:21:23 CEST - Created by HP OO. Change Order C
VM_LOCATION="DC1"
VCENTERNAME=
CLUSTER_NAME="ORACLE-DC1-T2-01"
HOST_NAME="
OS="Red Hat Enterprise Linux 7 (64-bit)"
CONFIGSFORHW="Red Hat Enterprise Linux 7 (64-bit)"
VMWARE_FOLDER="Linux\
SRM_PROTECTION="SRM protected (Synchronous Array-based Replication)"
```

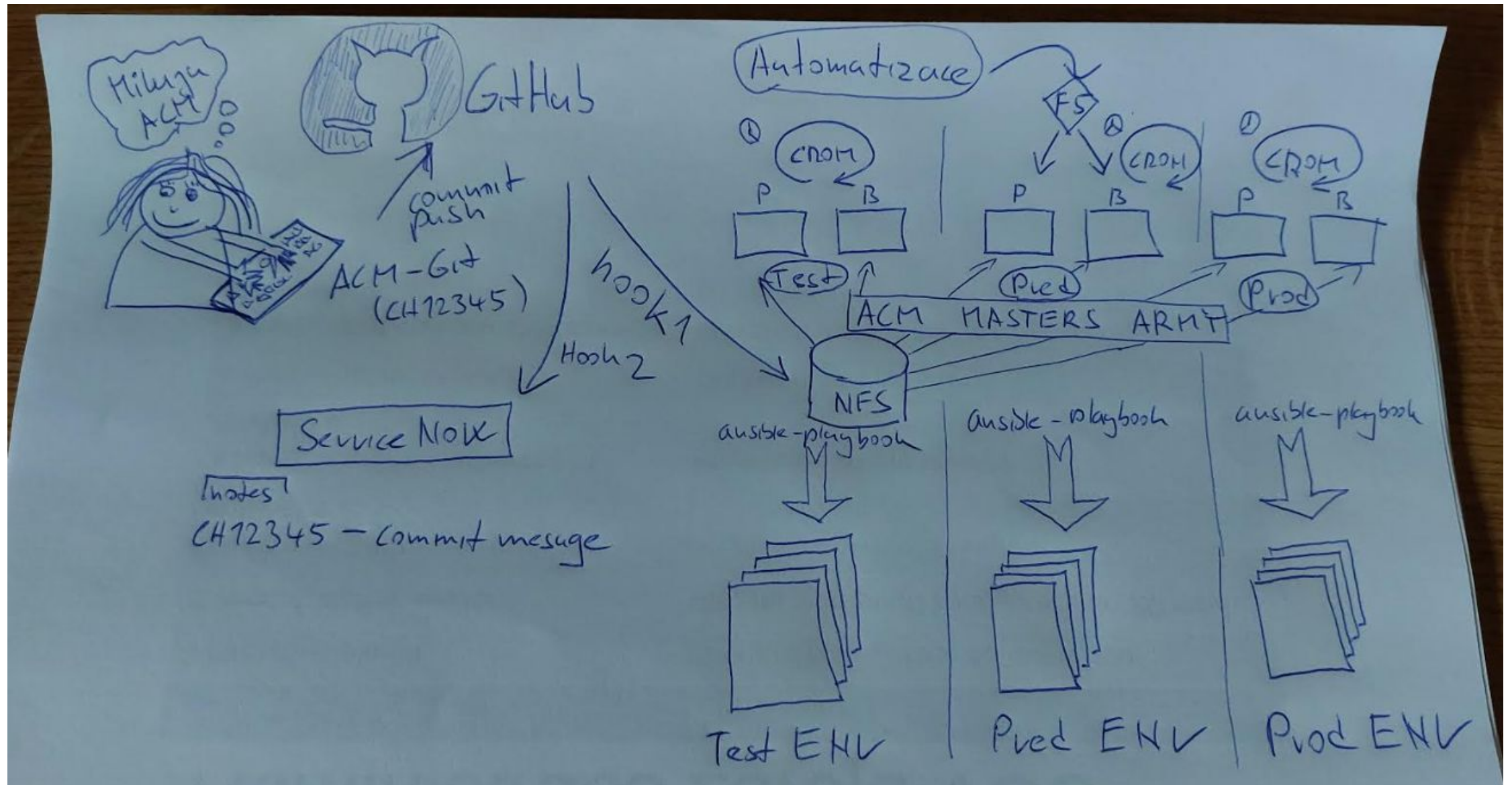
```
SRM_PROTECTION_GROUP="PG ORACLE-DC1-T2-01"
UUID="4213ac65-0b61- -84487e9918c5"
DISKENABLEUUID="TRUE"
VHW="vmx-13"

CM_GROUPS="acm_test,foreman_host_group_el7,foreman_host_group_el7_test,for
el7_test_db_oracle_norag,foreman_host_group_el7_test_db_oracle_norag.com

# Puppet compatible variables
CLUSTER="None"
STATUS="Alive"
ENVIRONMENT="Test"
ROLE="DB"
SOFTWARE="None"
PROJECT="INFRA"
FARM="None"
CONTACT="ithelpdesk@csas.cz"
CITY="Prague"
STREET=
DATA_CENTER="DC1"
```

```
(A) :~$
```

# ACM – architektura (HA)



# ACM – spouštění

- **Primárně jeden playbook na config. management co includeje role (viz výše)**
  - Ale používáme i další playbooku pod hlavičkou ACM
    - Správa clusterů, patching\_ready, ... (jednorázovky)
- Plánování cronem
  - Rozložení přes lokality
    - Když jedna vypadne "pouze" se prodlouží čas obrábění
- Role jsou rozdělené do skupin
  - Spouštění podle důležitosti
    - Csas\_epa (jednou za hodinu) vs. csas\_boot (jednou za 12 hodin)
- Runtime v kontejneru (Podman)
  - **Ansible runner (!)**
    - Samotný ansible je bohužel pomalý na takové množství práce

# ACM – a mnoho dalšího...

- Monitoring, logging, schedule, blacklisting, onboot-target, AWS/Tower/AAP/Umbrala, víc týmů, RBAC...
- ...ale na to už není čas. :-) Nebo jo?
- Ale tohle vypíchnout.
  - **Hromadná správa = zbraň hromadného ničení!!!**
    - Celkem jednoduše můžete způsobit **tmu**
    - Mějte nějak pořešený černý scénář, když si...
      - ...odstříhnete ssh přístup špatnou konfigurací
      - ...rozbijete sudo (nejde udělat změny pod rootem)
      - ...bohužel některé změny jsou nevratné... ale to víme.
        - Neprodáváme rohlíky...
- Nějak takhle to přibližně děláme my...



# laC – Outro

- Bude tedy s laC už všechno v klidu a míru?
  - zkuste a uvidíte... :-)
  - ... za rok to tu můžete odprezentovat.. :-)





# Díky za pozornost!

Dotazy, diskuze...

