# Silicon Hill

Informační systém klubu Silicon Hill

Bronislav Robenek, 2. Březen 2013

# Silicon Hill

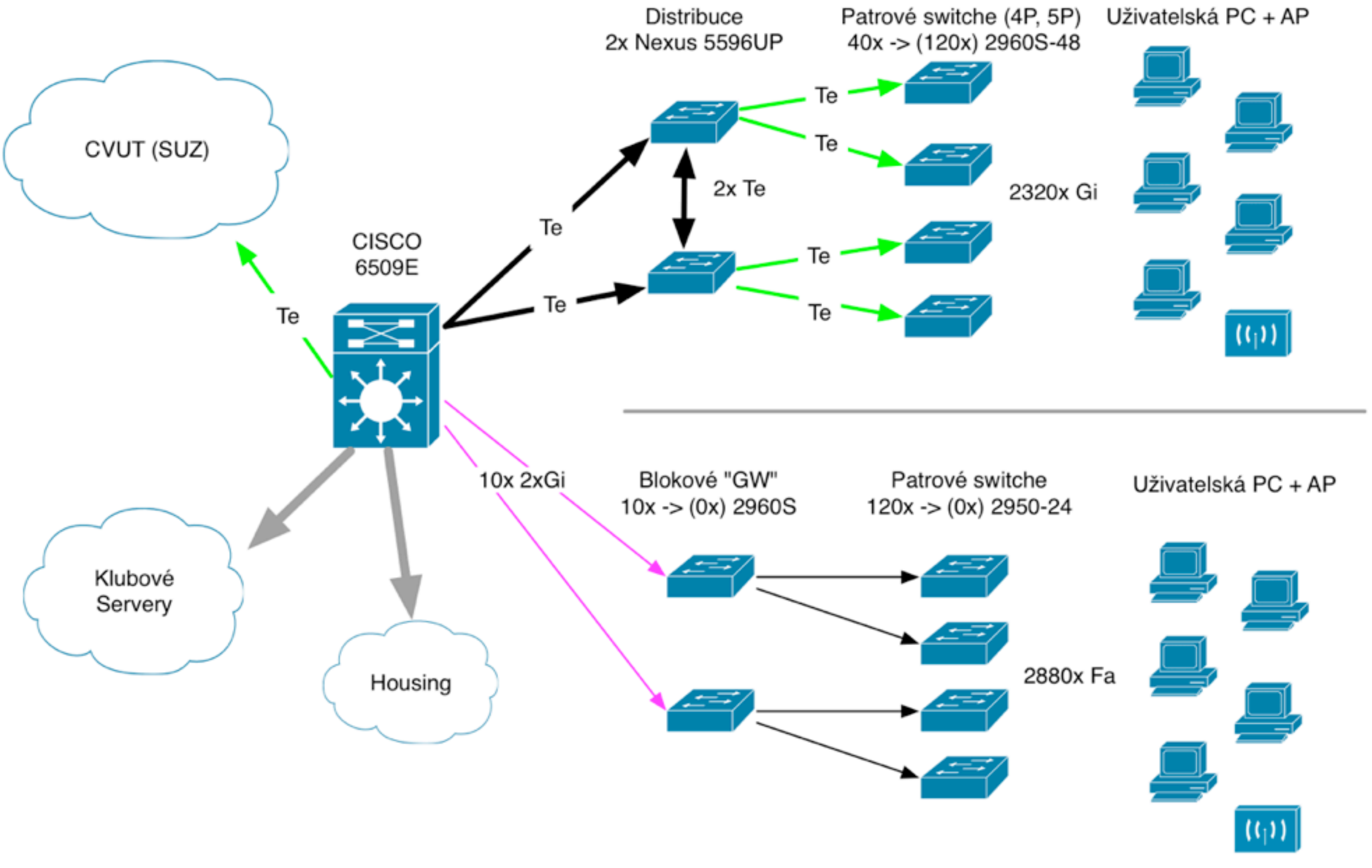
- Největší a zakládající klub SU ČVUT (1998 )

- Největší studenty spravovaná síť (začátky v 1993)

- 4256 členů
  4902 access portů
  35 AP
  (26.2.2013)

- Členské příspěvky

# L1


Distribuce
2x Nexus 5596UP
Patrové switche (4P, 5P)
40x -> (120x) 2960S-48
Uživatelská PC + AP
CVUT (SUZ)
CISCO
6509E
Te
Te
Te
Te
2x Te
Te
Te
Te
Te
2320x Gi
10x 2xGi
Blokové "GW"
10x -> (0x) 2960S
Patrové switche
120x -> (0x) 2950-24
Uživatelská PC + AP
Klubové
Servery
Housing
2880x Fa

# L2/L3 + MANAGEMENT

- 62 VLAN, na 1 VLAN ~ IPv4 + IPv6 subnet
- V celé síti 1 router - C6509E (ACL, NAT, PBR)
  `S*   0.0.0.0/0 [1/0] via 147.32.252.238`
- Access porty: port security + IP ACL

- Management síťových prvků
  - AAA: *tacacs+*
  - Záloha konfigurace: *rancid*
  - Logování: *syslog*
  - Monitoring: *nagios*

# ROZDĚLENÍ KOMPETENCÍ

- Síťová skupinka (~ 2) -> centrální prvky
- Serverová skupinka (~ 10) -> servery/služby
- Admini bloků (~ 10) -> blokové prvky
- Registrátoři (~ 80) -> uživatelské problémy
- **Informační systém řeší zbytek**

# ÚKOLY INFORMAČNÍHO SYSTÉMU

- Evidence uživatelů a zařízení
- Konfigurace síťových prvků (Port-sec + IP ACL)
- Přidělování adresního prostoru a doménových jmen
- Identifikace připojených zařízení a jejich historie
- Přiřazování členských příspěvků / Import z banky
- Dále: DNS, DHCP, SMTP, LDAP, RADIUS, Zálohy DB

# CO JSME TADY MĚLI?

# V ČEM BYL PROBLÉM?

- Neintuitivní a pomalé uživatelské rozhraní
  (vyhledání zařízení ~ 20s, časté chyby 500 - uživatel neví co se děje)
- Špatná validace a integrita dat
  - Duplicity uživatelských jmen a doménových názvů (10+ případů)
  - Háčky a hvězdičky v username (majda*, maťo)
  - Neplatná rodná čísla členů (5 případů)
    (Pro nás kritický údaj - identifikace členů občanského sdružení)
  - Nevalidní emaily (10+ případů)
- Konfigurace síťových prvků trvala dlouho, časté problémy (fretka)

# A ČÍM TO BYLO?

- Práce svépomoci + částečný outsourcing (2 roky vývoje, 6+ lidí, ~300k Kč)
  - Práce firmě zadávána pomocí tiketů, bez uceleného díla
  - Za výsledek odpovídala “domácí strana”
- Java?!
- Systém navrhovali a programovali síťaři a serveraři,  kteří neměli zkušenosti s vývojem aplikací
- Aplikační logika implementována ve složitých DB procedurách
  (Zbytečně složitá DB, zároveň však žádné constrainty)
- Žádná redundance ani monitoring kritických síťových služeb
  (Nejčastější problémem byl nedostatek volného místa na HDD)

# A CO TADY MÁME TEĎ?


## Přihlášení do IS

dominikmalis

Heslo

Přihlásit

Zapomněli jste heslo?

## Identifikace uživatele

| | |
|---|---|
| UID: | 19252 |
| Jméno: | Dominik Mališ |
| Username: | dominikmalis |
| Email: | d.malis@sh.cvut.cz |

## Registrátoři v okolí

| Pokoj | Jméno |
|---|---|
| Blok 6/52 | Michal Líska |
| Blok 6/233 | Kateřina Hašlarová |
| Blok 6/309 | Václav Mach |

## Základní informace o členství v klubu Silicon Hill

Členem klubu se můžete stát po registraci a zaplacení základního členského příspěvku. Registrace probíhá u registrátorů, kteří mohou do klubu přijímat pouze studenty vysokých škol bydlících na kolejích Strahov. Registrace ostatních fyzických osob probíhá v kanceláři klubu Silicon Hill. Podpisem registračního formuláře souhlasíte s interními předpisy a stáváte se členy občanského sdružení Studentská unie ČVUT.

### Nový informační systém!

Dne 1.10.2012 byl spuštěn nový informační systém. Je nutné aby si všichni uživatelé zaregistrováni před tímto datem resetovali heslo, použijte "Zapoměl jsem heslo" a váš SH mail. Bez resetu hesla nebude fungovat přihlášení na Wi-Fi, ani do dalších napojených systémů. Pro připomínky a hlášení chyb použijte systém pro hlášení chyb.

### Předregistrační formulář

Pro usnadnění registračního procesu vyplňte online předregistrační formulář a papírovou podobu registračního formuláře (šablony naleznete u registrátora). Následně navštivte registrátora s číslem předregistrace které vám vygeneruje systém, s předvyplněným registračním formulářem a s průkazem totožnosti (OP/Pas). Po registraci Vám bude přiděleno UID.

Předregistrační formulář

### Členské příspěvky

Po registraci a uhrazení členských příspěvků vám budou aktivovány odpovídající služby. Členské příspěvky se platí pouze bankovním převodem, složenkou nebo hotovostním vkladem v bance. Pro snadnější získání informací o platbě (ču/vs/ss/částka) využijte Kalkulátor příspěvků.

Kalkulátor příspěvků

# OKÉNKO DO HISTORIE

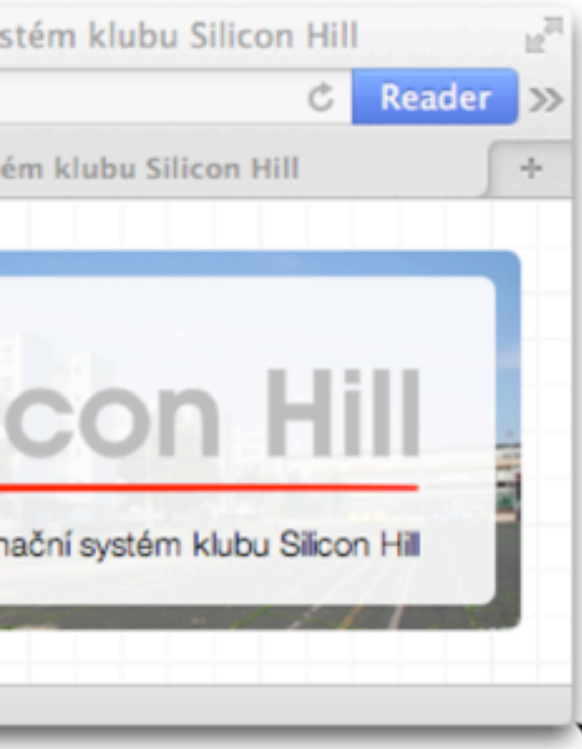
- 2001 - 2011 - Provoz DUSPS
- 2010 - Zahájení vývoje SUPP
- 9/2011 - Nasazení SUPP
- **6/2012 - Zahájení neveřejného vývoje IS**
- **8/2012 - IS představen vedení klubu**
- **1.10.2012 - Nasazení IS**

SUPP (http://cloc.sourceforge.net v 1.56) ./cloc.pl

| Language | files | blank | comment | code |
|---|---|---|---|---|
| Java | 461 | 10308 | 5913 | 32122 |
| HTML | 101 | 2592 | 1616 | 19018 |
| JSP | 178 | 1056 | 27 | 9779 |
| Javascript | 11 | 1292 | 1426 | 6614 |
| XML | 33 | 464 | 370 | 2243 |
| Bourne Shell | 22 | 121 | 262 | 325 |
| CSS | 2 | 26 | 11 | 90 |
| make | 2 | 19 | 7 | 29 |
| Objective C++ | 1 | 0 | 0 | 9 |
| Bourne Again Shell | 1 | 2 | 0 | 4 |
| SUM: | 812 | 15880 | 9632 | 70233 |

IS (http://cloc.sourceforge.net v 1.56) ./cloc.pl --force-lang=HTML,erb

| Language | files | blank | comment | code |
|---|---|---|---|---|
| Ruby | 327 | 2278 | 1690 | 12691 |
| HTML | 285 | 781 | 65 | 6681 |
| Javascript | 7 | 236 | 242 | 1543 |
| YAML | 43 | 50 | 46 | 1210 |
| CSS | 4 | 133 | 15 | 885 |
| CoffeeScript | 1 | 0 | 0 | 4 |
| SUM: | 667 | 3478 | 2058 | 23014 |




PostgreSQL

Materialized views

Read Only SQL

POWERDNS

DNS Server/Recursor/Cache

ISC DHCP + Patch

POSTFIX

SMTP Server

pgboucner

R/W SQL

HTTPS

SSH

Model

View/Controller

Workery
(Delayed Job)

IS Applikace

Síťové prvky

R/W LDAP

OpenDJ

LDAP Server

RO LDAP

freeRADIUS

RADIUS Server

# CO BYLO KLÍČEM?

- Vývoj ve dvou lidech - utajený až do vertikálního představení
- Ruby on Rails ekosystém
- Zkušenost autorů s menšími i srovnatelnými projekty
- Věděli jsme přesně co chceme - kvalitní návrh
- Do databáze se zapisuje pouze přes model aplikace, který vše validuje ( => integrita).
- HA již od začátku (např. fotky uživatelů)

# RUBY ON RAILS EKOSYSTÉM

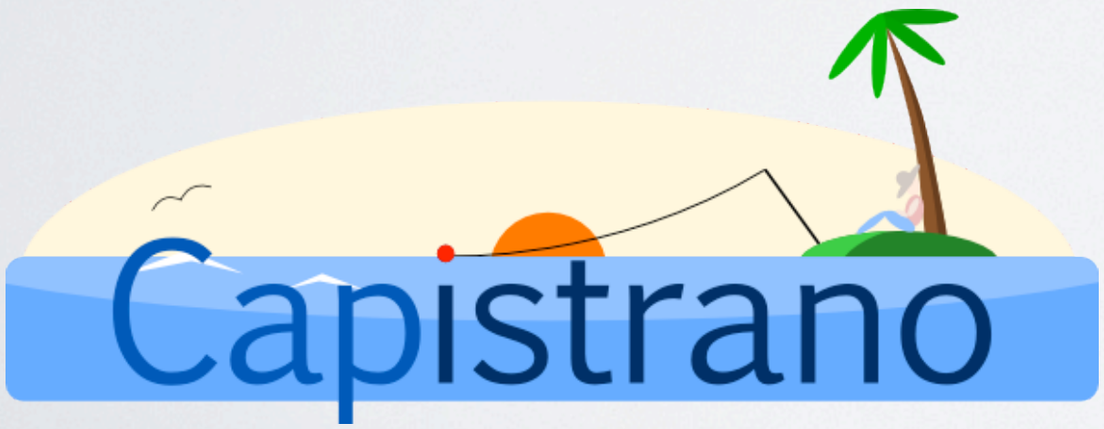

http://www.ruby-lang.org/


http://rubyonrails.org

Thin

http://code.macournoyer.com/thin/


http://godrb.com

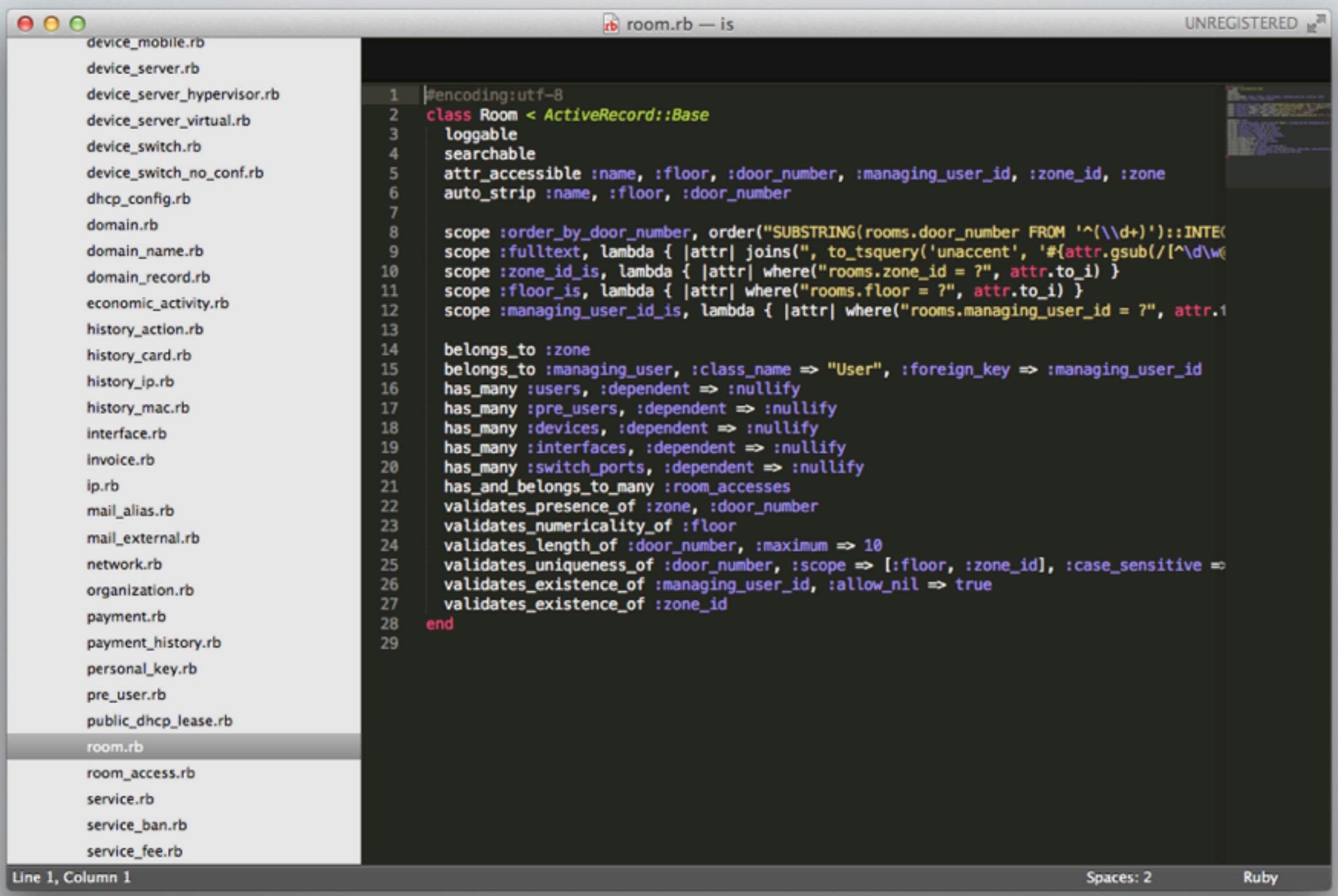



https://github.com/capistrano/capistrano

**Delayed::Job**

https://github.com/collectiveidea/delayed_job

# UKÁZKA #1


room.rb — is
UNREGISTERED
device_mobile.rb
device_server.rb
device_server_hypervisor.rb
device_server_virtual.rb
device_switch.rb
device_switch_no_conf.rb
dhcp_config.rb
domain.rb
domain_name.rb
domain_record.rb
economic_activity.rb
history_action.rb
history_card.rb
history_ip.rb
history_mac.rb
interface.rb
invoice.rb
ip.rb
mail_alias.rb
mail_external.rb
network.rb
organization.rb
payment.rb
payment_history.rb
personal_key.rb
pre_user.rb
public_dhcp_lease.rb
room.rb
room_access.rb
service.rb
service_ban.rb
service_fee.rb
#encoding:utf-8
class Room < ActiveRecord::Base
loggable
searchable
attr_accessible :name, :floor, :door_number, :managing_user_id, :zone_id, :zone
auto_strip :name, :floor, :door_number
scope :order_by_door_number, order("SUBSTRING(rooms.door_number FROM '^(\\d+)')::INTE
scope :fulltext, lambda { |attr| joins(", to_tsquery('unaccent', '#{attr.gsub(/[^\d\w
scope :zone_id_is, lambda { |attr| where("rooms.zone_id = ?", attr.to_i) }
scope :floor_is, lambda { |attr| where("rooms.floor = ?", attr.to_i) }
scope :managing_user_id_is, lambda { |attr| where("rooms.managing_user_id = ?", attr.1
belongs_to :zone
belongs_to :managing_user, :class_name => "User", :foreign_key => :managing_user_id
has_many :users, :dependent => :nullify
has_many :pre_users, :dependent => :nullify
has_many :devices, :dependent => :nullify
has_many :interfaces, :dependent => :nullify
has_many :switch_ports, :dependent => :nullify
has_and_belongs_to_many :room_accesses
validates_presence_of :zone, :door_number
validates_numericality_of :floor
validates_length_of :door_number, :maximum => 10
validates_uniqueness_of :door_number, :scope => [:floor, :zone_id], :case_sensitive =>
validates_existence_of :managing_user_id, :allow_nil => true
validates_existence_of :zone_id
end
Line 1, Column 1
Spaces: 2
Ruby

# POUČENÍ #1

- Vyvíjejte sami, nebo zadejte celý projekt firmě
- Od jednoduššího k složitějšímu
- Neprogramujte v Javě pokud vás za to neplatí
  (nebo pokud potřebujete multiplatformní desktopovou aplikaci)
- Vyhněte se procedurám v databázi
  (pokud to nedotáhnete do konce a nezdokumentujete)
- Dejte přednost ekosystému před jazykem
- Vyvíjejte, neschůzujte (RAD)

# VYSOKÁ DOSTUPNOST

- Řešíme SPOF (Single point of failure)
- Cílem je "aby se to samo nepokazilo" => **Prevence**
  => monitoring (trendy, ...) -> *Munin*
  => včasné varování (místo na disku, ...) -> *Nagios*
- Systém by si, ale "měl poradit sám" => **Redundance**
  => fail over + [load balancing]
  => replikace dat
  => fencing

# PACEMAKER

- *Pacemaker* = Cluster manager
  (http://clusterlabs.org , http://www.corosync.org)
- *Node* = Server, několik serverů je ve společném clusteru
  (rozhoduje  zvolený master; komunikace Corosync)
- *CIB* = Cluster Information Base
  (konvergovaný stav - všechny nody ví všechno = konfigurace a stav)
- *Resource* = "služba", například IP adresa, nebo proces
- *Resource Agent* (RA) = "wrapper" kolem konkrétní služby
  (parametrizovaný SH skript - start, stop, ...)

# PACEMAKER - KONFIGURACE

- Definice služeb (RA, parametry)

```
primitive ip1 ocf:heartbeat:IPaddr2 params ip="1.2.3.4" cidr_netmask="24"
```

- Kde může která služba běžet (primitve, score, node)

```
location loc_ip1_node1 ip1 100: node1
```

- Kolikrát má služba běžet v clusteru (primtive, počet)

```
clone nginx nginxd meta clone-max="2"
```

- Logické uspořádání služeb

```
group pgsql fs_pgsql ip_pgsql pgsqld
colocation ip1_on_nginx inf: ip_1 nginx
```

- Pořadí spouštění služeb

```
order nginx_after_ip inf: ip1 nginx
```

# GOV 1

# GOV 2

NGINX load balancer
is.sh.cvut.cz
+ ssl offload

NGINX load balancer
static.is.sh.cvut.cz

NGINX pro assets

IS 1

thin 3
thin 2
thin 1
worker 3
worker 2
worker 1
assets

IS 2

thin 3
thin 2
thin 1
worker 3
worker 2
worker 1
assets

LDAP 1

RADIUS

LDAP 2

RADIUS

SVC 1

PowerDNS

ISC DHCPD
+ SH DBI Patch

SMTP (Postfix)

SVC 2

PowerDNS

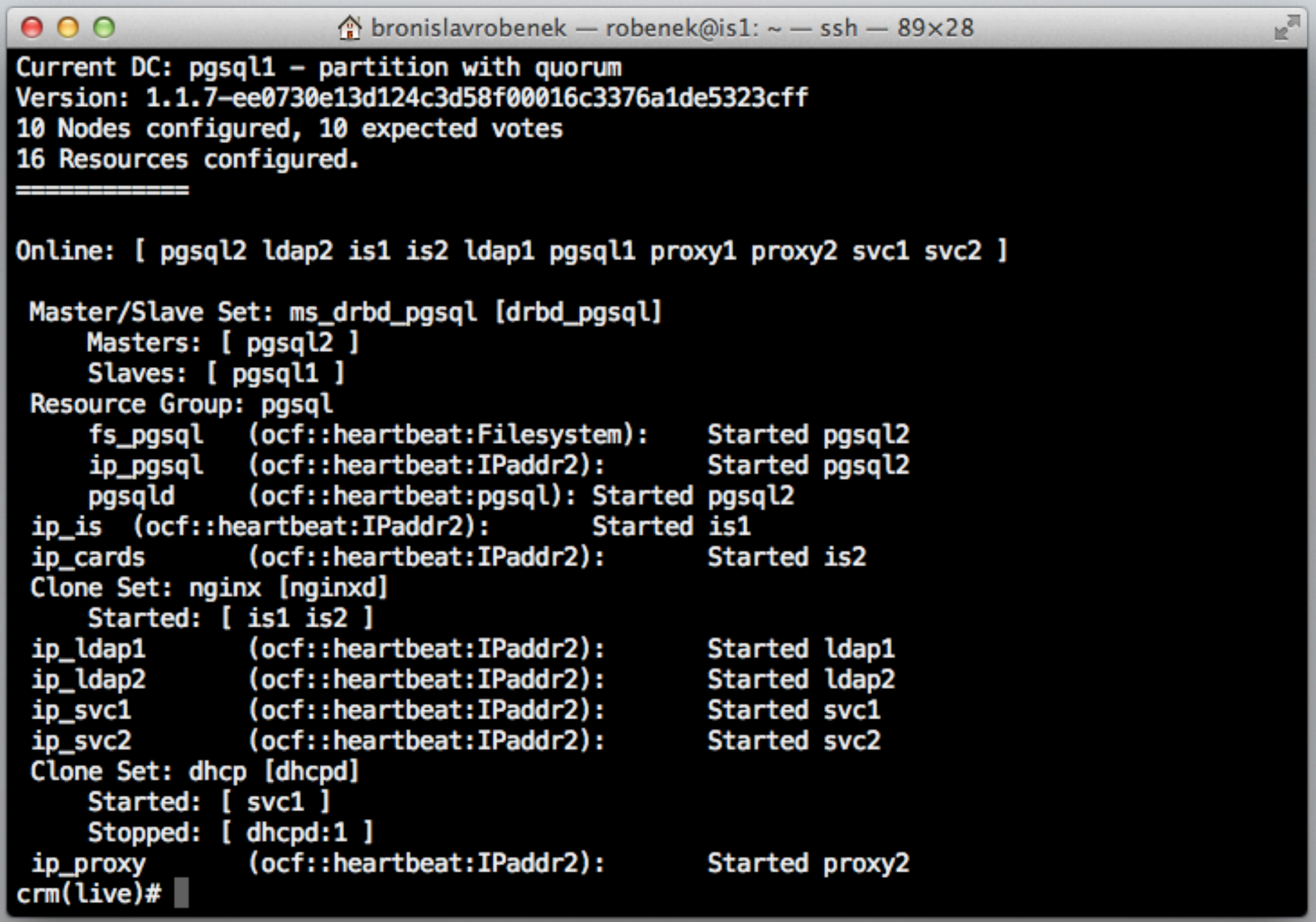
ISC DHCPD
+ SH DBI Patch

SMTP (Postfix)

PGSQL 1

PGSQL 2

# UKÁZKA #2


bronislavrobenek — robenek@is1: ~ — ssh — 89×28
Current DC: pgsql1 - partition with quorum
Version: 1.1.7-ee0730e13d124c3d58f00016c3376a1de5323cff
10 Nodes configured, 10 expected votes
16 Resources configured.
Online: [ pgsql2 ldap2 is1 is2 ldap1 pgsql1 proxy1 proxy2 svc1 svc2 ]
Master/Slave Set: ms_drbd_pgsql [drbd_pgsql]
Masters: [ pgsql2 ]
Slaves: [ pgsql1 ]
Resource Group: pgsql
fs_pgsql (ocf::heartbeat:Filesystem): Started pgsql2
ip_pgsql (ocf::heartbeat:IPaddr2): Started pgsql2
pgsqld (ocf::heartbeat:pgsql): Started pgsql2
ip_is (ocf::heartbeat:IPaddr2): Started is1
ip_cards (ocf::heartbeat:IPaddr2): Started is2
Clone Set: nginx [nginxd]
Started: [ is1 is2 ]
ip_ldap1 (ocf::heartbeat:IPaddr2): Started ldap1
ip_ldap2 (ocf::heartbeat:IPaddr2): Started ldap2
ip_svc1 (ocf::heartbeat:IPaddr2): Started svc1
ip_svc2 (ocf::heartbeat:IPaddr2): Started svc2
Clone Set: dhcp [dhcpd]
Started: [ svc1 ]
Stopped: [ dhcpd:1 ]
ip_proxy (ocf::heartbeat:IPaddr2): Started proxy2
crm(live)#

# POUČENÍ #2

- Starat se o selhání systému nebo se raději starat o cluster? Vždy je potřeba odpovědná osoba!
- Konfigurace není z pravidla modulární, to co funguje někde, nebude fungovat u vás.
- Největším problémem byla databáze, proto jsme skončili s řešením pomocí DRBD.
- Pacemaker nám umožnil zero downtime při upgrade HW, SW a testování.
- Dohled nás zachránil cca 7x, Pacemaker cca 2x

# ZÁVĚR

- Ano, takový systém se dá vyvinout za 15 víkendů.
- Doufáme, že se najdou mladší členové, kteří to posunou zase o krok dál.
- Od nasazení nebyl jediný výpadek DHCP a DNS.
- Do budoucna: DNSSEC, IPv6, Anglická verze

# AUTOŘI A PODĚKOVÁNÍ

- Bronislav Robenek <b.robenek@sh.cvut.cz>
  (HA, model, DNS, DHCP)
- Dominik Mališ <d.malis@sh.cvut.cz>
  (RoR aplikace, model, konfigurace prvků)
- Tomáš Srna <t.srna@sh.cvut.cz>
  (Konfigurace: LDAP, RADIUS a SMTP serverů)
- Dále:
  Viktor Bohuslav Bohdal,
  Kateřina Hašlarová