

eduroam.cz

správa a deployment pomocí Ansible

Jan Tomášek <semik@cesnet.cz>

oddělení síťové identity / CESNET

uživatelská jména v **eduroamu**:

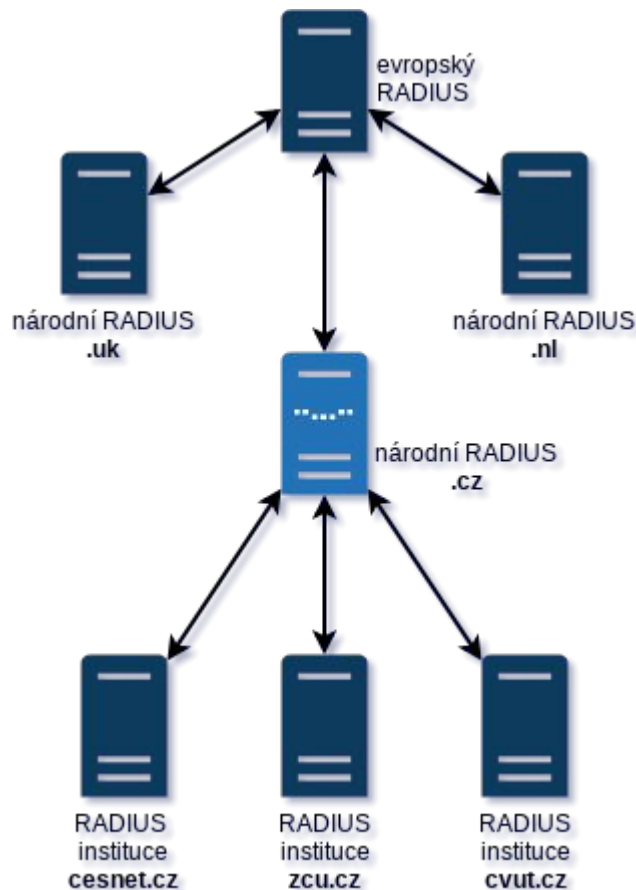
uživatel@realm

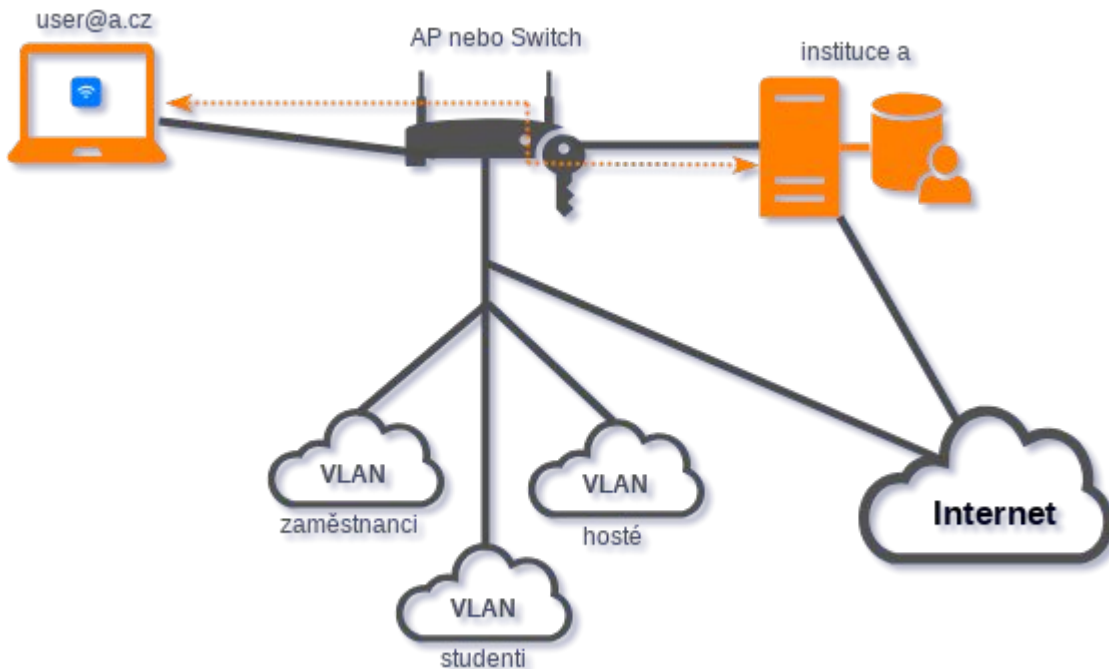
např.:

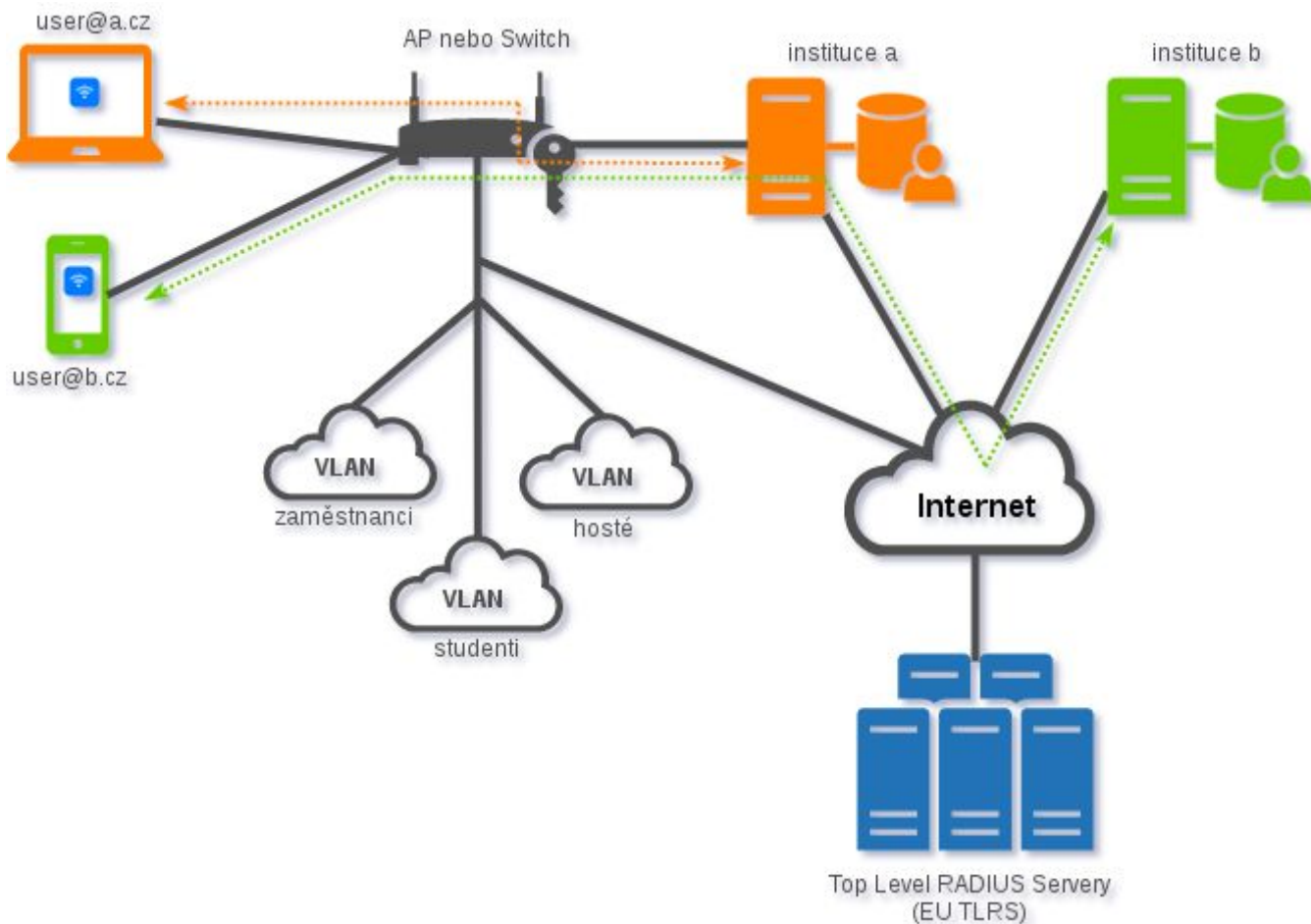
semik@cesnet.cz

helmut@dfn.de

realm [relm], ~~Eduroam~~, ~~eduRoam~~, ~~EDUROAM~~







Ansible usnadňuje znovupoužitelnost konfigurací a správu většího množství serverů

národní RADIUS jsou dva DELL PE 630 servery

pár (<10) institucí využívá službu freeRADIUS ve správě CESNETu

<https://github.com/CESNET/ansible-freeradius>

Ansible je také skvělá dokumentace a záloha

playbook pro nasazení freeRADIUSu pro připojení k eduroamu v ČR:

<https://github.com/CESNET/ansible-freeradius>

důvěrné informace ve vaultu

playbook pro nasazení freeRADIUSu pro připojení k eduroamu v ČR:

<https://github.com/CESNET/ansible-freeradius>

důvěrné informace ve vaultu, diff:

```
131 35376661633034376165306166336361383839666437623765656538613361343735623137663639
132 34336434623737326230333533613066633663373635313135326637326530653138626437333235
133 30663437306132303537633937653361333835636330346233616161333236383232643731356138
134 61656561363736653863656636636131616465393834633935333566323337333135643431643265
135 35333962376634656336636536613565663531323162303237656236666364313233356464386662
136 39373961356130303039646661363837613763316566336639613063336262303632326463373963
137 39303131326639393438326535643636376262373164373166623563323037666266666431613331
138 36653730623331313534636131306333373164346539336562633637633035323634613662363364
139 63653431353163386235663832336161353164663766663763326262313866323264623564663165
140 306438303338333466666162353465316264333465346232616132376166637346439326166303039
141 33346266333139326636656165633738356239663262613764643431616535646362333430623434
142 65663731333262336131316465656234326334393361306534656234656532326230623534353961
143 63306263346339303330333235656631636333303361356433353736303936383038626662303334
144 34643135623536623036663230366535353033643664623462613737663666303433623063316163
145 34636532303461656566
2 63343439363137343634373466363337636430656137623631343761646135326437666433366534
3 3234373161663361653463396466613164353266373134620a353165623763356435313066366636
4 66663662373366353732663936646266393130376632393138653566376534333362636334373836
5 3234313736306465350a303836373236663731626462376235353834303661366364323536666638
6 3035623262336333634313435633937663632666362373633316535343934396230306437316333
7 38343538363532363866376564643264656365373961316462373432363061383930353862313833
8 38356231396239646233373731336564353830356633386434386665666338363230333564386665
9 64393032653963643234626162333664636461326236616438633965633764333731393538613832
10 36626138633533346134383961393762316161636266313135353039303966336265313731303164
11 61373532626163613839396366376233343932386165323235643031656536656664653837643332
12 39353961616131393262386563626130316236656265353337303763383064353437363236343962
13 36313438326139393964636261646261303065623365626463396566626639666263656461666366
14 383863663634376538613666633383435313935636463383436336639633766623438653361366239
15 37373836313664376464373165626261666630663934346632653265383336636438623165303463
```

```
semik@semik4:~/proj/aaai [master✓]✓$ ls -l host_vars/*.yaml
```

```
host_vars/radius.org1.cz-vault.yaml
```

```
host_vars/radius.org1.cz.yaml
```

```
host_vars/radius.org2.cz-vault.yaml
```

```
host_vars/radius.org2.cz.yaml
```

```
semik@semik4:~/proj/aaai [master✓]✓$ cat playbook-freeradius.yaml
```

```
...
```

```
- name: load variables
```

```
  hosts: eduroam-managed
```

```
  tasks:
```

```
    - include_vars: "host_vars/{{ inventory_hostname }}-vault.yaml"
```

```
...
```

```
semik@semik4:~/proj/aaai [master✓]✓$ ansible-playbook playbook-freeradius.yaml \
  --vault-password-file vault_eduroam_managed.txt
```


eduConfigurator.pl

```
emacs@doma.doma.tomasek.cz
File Edit Options Buffers Tools Help

TLS_Protocols TLSv1, TLSv1.1, TLSv1.2
TLS_CAPath /etc/ssl/certs
TLS_CertificateFile ".$config->newCert."
TLS_CertificateType PEM
TLS_PrivateKeyFile ".$config->newKey."
TLS_CRLCheck
TLS_CRLFile /etc/ssl/crl/*.r0\n".
useTLS_ExpectedPeerName($hostname).

$keepaliveTimeout
NoreplyTimeout 8

NoReplyHook sub { DeadRealm::noReplyHook(\@); };
ReplyHook sub { DeadRealm::replyHook(\@); NREN::stripAttrs(\@); NREN::patchAccounting(\@); };
StripFromRequest eduroam-SP-Country$stripONandCUI
</AuthBy>\n\n";

$radiuses{$radius->dn}->{single_authby} = " #Host $hostname
Host ".$getIP($hostname).
Secret ".$radiuses{$radius->dn}->{secret}."

MaxFailedRequests 1000
MaxFailedGraceTime 360
FailureBackoffTime 1

LocalAddress ".$getIP($config->LocalName).

TLS_Protocols TLSv1, TLSv1.1, TLSv1.2
TLS_CAPath /etc/ssl/certs
TLS_CertificateFile ".$config->newCert."
TLS_CertificateType PEM
TLS_PrivateKeyFile ".$config->newKey."
TLS_CRLCheck
TLS_CRLFile /etc/ssl/crl/*.r0\n ".
useTLS_ExpectedPeerName($hostname).

$keepaliveTimeout
NoreplyTimeout\t8

ReplyHook\t\tsub { NREN::stripAttrs(\@); NREN::patchAccounting(\@); };
StripFromRequest\teduroam-SP-Country$stripONandCUI\n";
} else {
die "Unknown transport method = $transport\n";
};
};

my %publishClients;
my %publishDeadRealmHostDefinitions;

-:--- eduConfigurator.pl 48% L473 Git-master (Perl)
```

radius.cfg

```
emacs@doma.doma.tomasek.cz
File Edit Options Buffers Tools Conf Help

# This definition is used 1 times.
<AuthBy RADSEC>
Identifier radius1.cesnet.cz

MaxFailedRequests 3 # 5
MaxFailedGraceTime 30 # 360
FailureBackoffTime 30 # 1

#Host radius1.cesnet.cz
Host 195.113.144.226
Secret radsec

LocalAddress 195.113.187.22

TLS_Protocols TLSv1, TLSv1.1, TLSv1.2
TLS_CAPath /etc/ssl/certs
TLS_CertificateFile /etc/ssl/certs/radius1.eduroam.cz.crt
TLS_CertificateType PEM
TLS_PrivateKeyFile /etc/ssl/private/radius1.eduroam.cz.key
TLS_CRLCheck
TLS_CRLFile /etc/ssl/crl/*.r0
CertificateAltNameDNS radius1.cesnet.cz
CertificatePeerName CN=radius1.cesnet.cz(|emailAddress=.)$

$keepaliveTimeout 29
NoreplyTimeout 8

NoReplyHook sub { DeadRealm::noReplyHook(\@); };
ReplyHook sub { DeadRealm::replyHook(\@); NREN::stripAttrs(\@); NREN::patchAccounting(\@); };
StripFromRequest eduroam-SP-Country
</AuthBy>

# This definition is used 3 times.
<AuthBy RADSEC>
Identifier radius1.cuni.cz

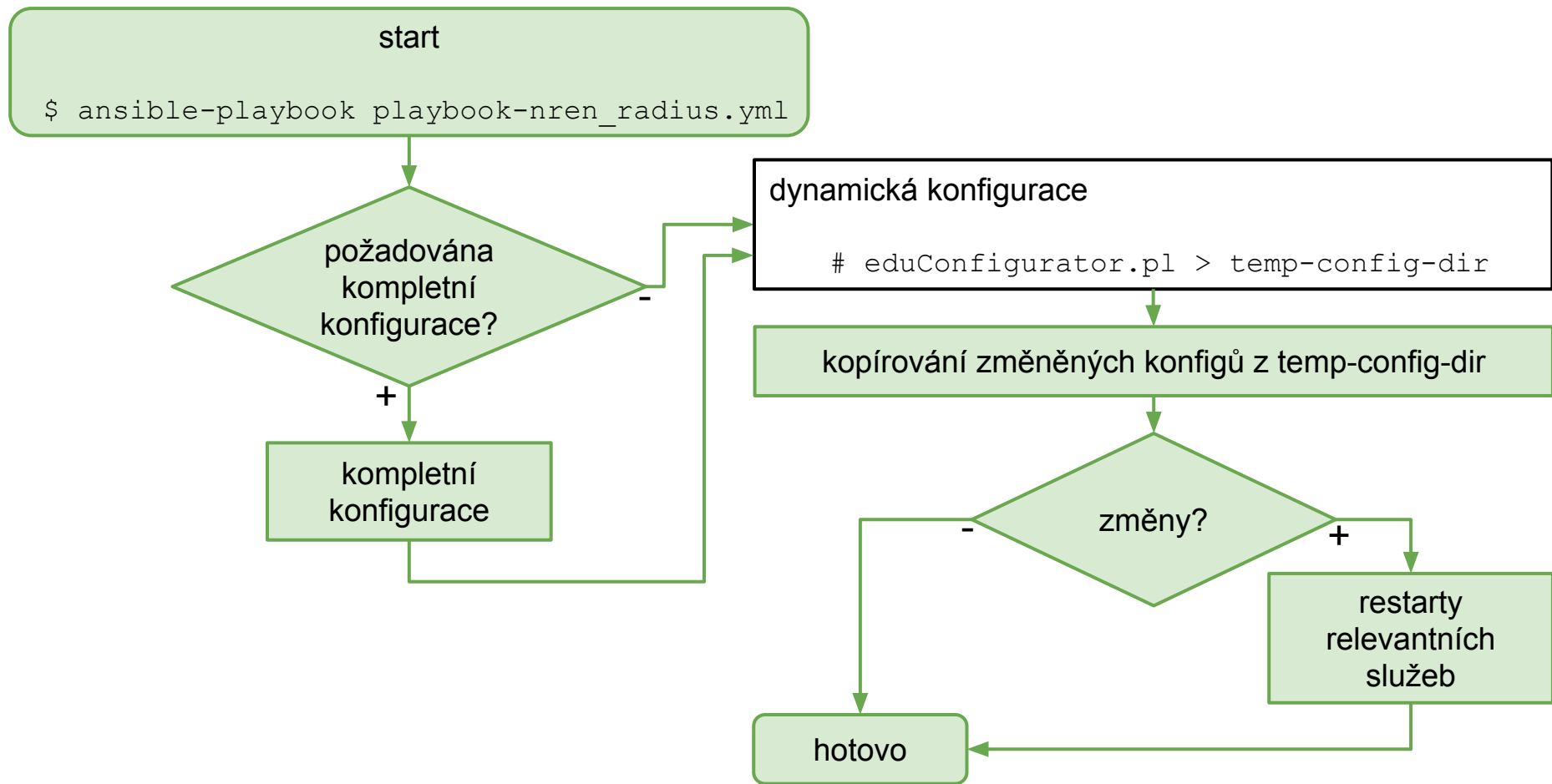
MaxFailedRequests 3 # 5
MaxFailedGraceTime 30 # 360
FailureBackoffTime 30 # 1

#Host radius1.cuni.cz
Host 195.113.0.250
Secret radsec

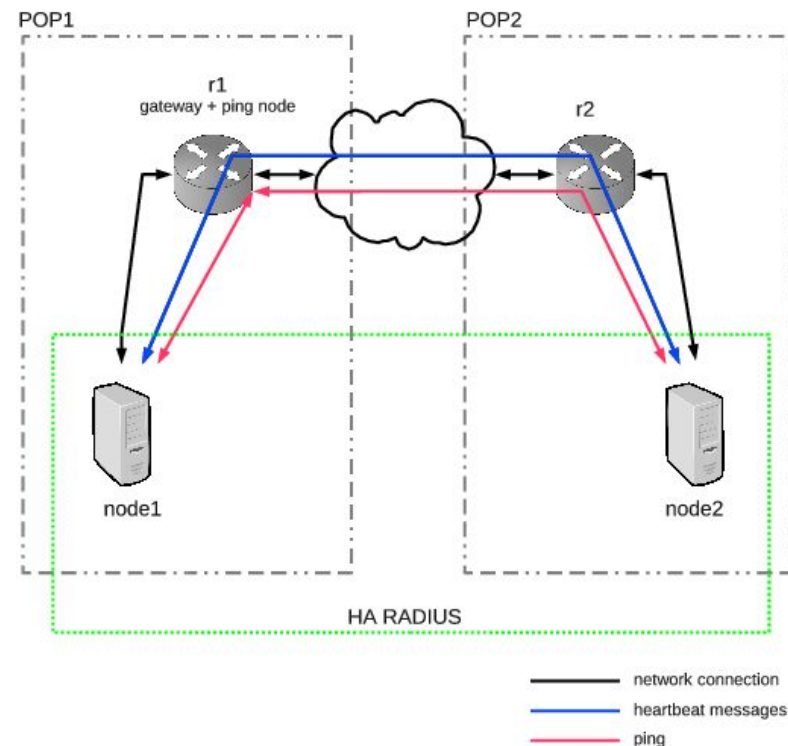
LocalAddress 195.113.187.22

TLS_Protocols TLSv1, TLSv1.1, TLSv1.2
TLS_CAPath /etc/ssl/certs
TLS_CertificateFile /etc/ssl/certs/radius1.eduroam.cz.crt

-:--- radius-auto.conf 15% L138 (Conf[Space])
```



- do cca 2009 dva nezávislé RADIUS servery
 - spousty chybně nainstalovaných RADIUSů
- první cluster postavený pomocí heartbeatu
 - už v té době zastaralý, ale jednoduchý
 - aktivní + záložní uzel
 - oddělené lokality, ale závislé na L2
 - v provozu 2009 - 2017
 - [CESNET technical report 23/2009](#)



- v současnosti používáme corosync + pacemaker ['pās ,mākər]
- stále máme dva uzly (aktivní + záložní)
 - všech 10 zdrojů musí být na jediném uzlu

```
root@radiuslmng4:~# crm status
```

```
...
```

```
Full list of resources:
```

```
Clone Set: clone_ping_gw [ping_gw]
```

```
Started: [ radiuslmng4 radiuslmng5 ]
```

```
Resource Group: group_eduroam.cz
```

```
nren_ip      (ocf::heartbeat:IPaddr2):    Started radiuslmng4
```

```
d_radsec_ip  (ocf::heartbeat:IPaddr2):    Started radiuslmng4
```

```
offline_file (systemd:offline_file):      Started radiuslmng4
```

```
racoon       (systemd:racoon):             Started radiuslmng4
```

```
radiator     (systemd:radiator):           Started radiuslmng4
```

```
eduroam_ping (systemd:eduroam_ping):       Started radiuslmng4
```

```
icinga2      (systemd:icinga2):             Started radiuslmng4
```

```
mailto       (ocf::heartbeat:MailTo):       Started radiuslmng4
```

```
semik@semik4:~/proj/aaai [master✓]✓$ ansible-playbook playbook-nren_radius.yml  
--extra-vars full_config=1
```

```
semik@semik4:~/proj/aaai [master✓]✓$ cat roles/nren_radius/tasks/main.yml
```

```
...  
- name: uvedeni zalozniho uzlu do standby modu  
  include: disable_slave.yml  
  when: not ONLINE and full_config|bool  
...  
- name: konfigurace corosyncu  
  include: corosync.yml  
  when: full_config|bool  
...  
- name: konfigurace pacemakeru  
  include: cluster.yml  
  when: not ONLINE and full_config|bool  
...  
- name: uvedeni zalozniho uzlu do online modu  
  include: enable_slave.yml  
  when: not ONLINE and full_config|bool
```


konfigurace corosync-u se sestává z

- nakopírování template corosync.conf.j2

- vytvoření a roz distribuování /etc/corosync/authkey

pacemaker se konfiguruje sekvencí volání přes Ansible command

- neuspokojivý stav modulů

- parsování výstupů cli

informace o jednotlivých zdrojích ve skupinovém inventory

jen dva uzly - možnost split-brain

nemáme žádná uživatelská data, jen přehazujeme pakety

přestože je uzel standby, při konfiguraci exportuje změněnou konfiguraci

doba restartu (~30s) zdroje radiator způsobuje zbytečné migrace

ochrana před duplicitním spuštěním dvěma správci najednou
fragment playbooku: <http://tomasek.cz/LD18/zamykani.yml>

zámek:

```
root@radiuslmng4:~# cat /tmp/ansible-playbook.lock
2018.09.26 12:46:58 Blame -> lager@192.0.2.105 2001:db8::105
SSH_CONNECTION='192.0.2.105 38962 195.113.187.36 22'
```

záznam v syslogu:

```
Sep 26 12:46:58 radiuslmng4 root[16101]: Ansible executed by lager@192.0.2.105
2001:db8::105 SSH_CONNECTION='192.0.2.105 38962 195.113.187.36 22'
```

podklady získáváme z ``whoami` & `hostname --all-ip-addresses``

ochrana před spuštěním starého playbooku

```
pre_tasks:
```

```
...
```

- name: fetch current state of repository

```
local_action: command git fetch
```

```
changed_when: false
```

- name: get repository status

```
local_action: command git log HEAD..origin
```

```
register: git
```

```
changed_when: false
```

- name: ask user to continue if local repository is not up to date

```
pause:
```

```
  prompt: "lokalni repozitar neni aktualni. Pokracovat?"
```

```
register: continue
```

```
when: git.stdout != ""
```

eduroam.cz

správa a deployment pomocí **Ansible**

Otázky?

semik@cesnet.cz

Hledáme nové kolegy:

- správce a vývojář internetových služeb
- analytik digitální forenzní laboratoře
- správce a vývojář multimediálních služeb

Více informací na stránku sdružení CESNET
a nebo na [webu](#).