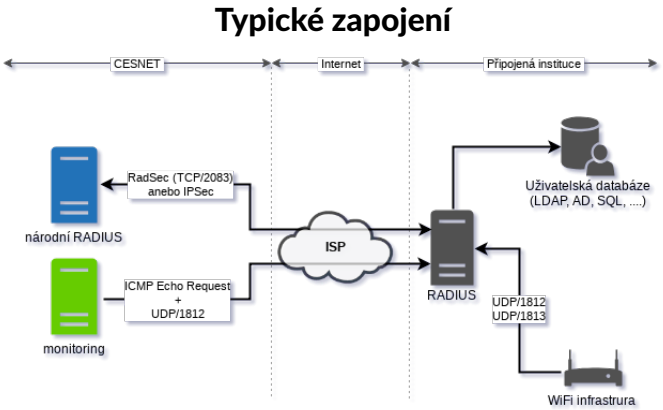
eduroam.cz - monitoring infrastruktury a detekce problémů

Václav Mach

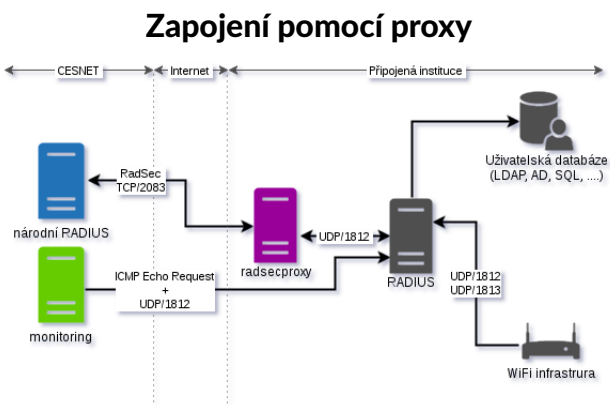
cesnet

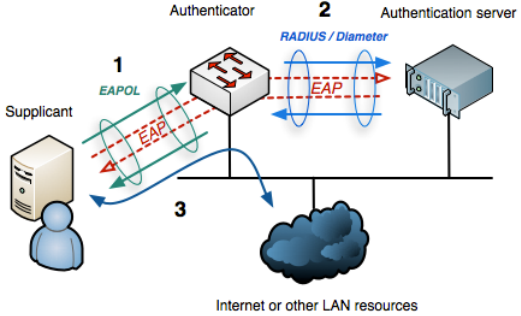
7. října 2018

Základní zapojení institucí



Základní zapojení institucí



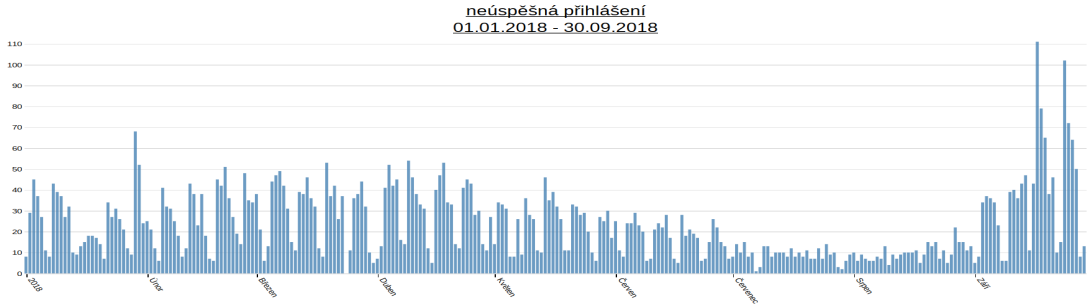



```
*** Received from 78.128.211.146 port 39342 ....
Code: Access-Request
Identifier: 108
Attributes:
        User-Name = "semik@cesnet.cz"
        Called-Station-Id = "F4-F2-6D-22-71-44:eduroam"
        NAS-Port-Type = Wireless-IEEE-802-11
        NAS-Port = 2
        Calling-Station-Id = "XX-XX-XX-XX-XX-XX"
        Connect-Info = "CONNECT 54Mbps 802.11g"
        Acct-Session-Id = "5BA7CE53-00000010"
        Framed-MTU = 1400
        Operator-Name = "1eduroom.cesnet.cz"
        Chargeable-User-Identity = <0>
        Proxy-State = OSC-Extended-Id=1388
```

Když to nefunguje … tak to někdo opraví?

Přestože jde o ”jednoduchuše” fungující službu, existuje mnoho různých věcí, které můžou zapříčinit nefunkčnost pro koncové uživatele:

- nefunkční spojení na národní RADIUS – nemožné ověření návštěvníků
- různorodé bugy v RADIUS serverech
- špatné SSID (např **E**duroam)
- špatné uživatelské jméno (`user@seznam.cz`, `”user@realm.cz ”`, …)



Proč monitorovat

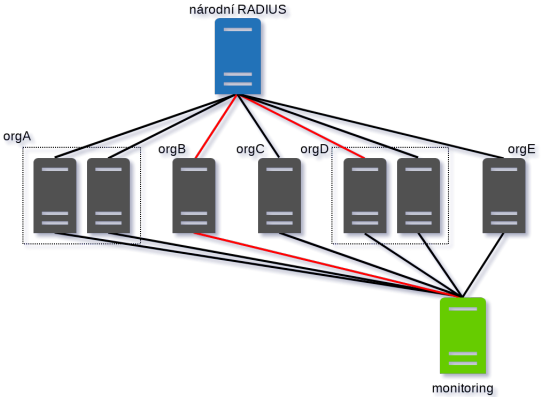
Monitorujeme, protože je lepší přijít na problém dřív než uživatel.

- nefunkčnost kazí dojem kvalitní služby
- řada uživatelů se nikdy s problémem neozve
- uživatelé mnohokrát nejsou schopni poskytnout relevantní informace
- některé problémy jsou specifické pro určité IdP & SP
- některé problémy představují bezpečnostní riziko

cesnet

Dřívější a současný stav monitoringu

Stroj v rámci eduroam infrastruktury, který simuluje přístupový bod (AP).



Existují i HW sondy, ale jsou používány pouze v lokálním měřítku.

cesnet

Dřívější stav monitoringu

- v provozu od roku 2006
- jádrem byl nagios 2, dále přechod na nagios 3
- staticky generovaná konfigurace
- `http://archiv.cesnet.cz/doc/techzpravy/2006/eduroam-monitoring/`

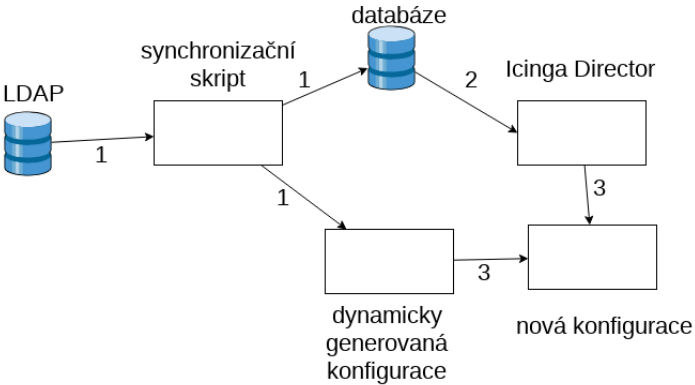
cesnet

Nový stav monitoringu

- v provozu od září 2018 (vývoj od Q1 2018)
- jádrem je Icinga 2
- cílem byla kompletně dynamická konfigurace bez staticky generovaných částí
- část konfigurace musí být generována kvůli problémům s directorem
- odstraněna pevná závilost na zdroji dat
- synchronizaci zajišťuje Icinga director, fileshipper a vlastní synchronizační skript

cesnet

Nasazování konfigurace



1. kontrola dostupnosti nových dat, vložení do databáze, generování konfigurace
2. synchronizace Directora z databáze
3. nasazení všech částí do celkové konfigurace

cesnet

Nasazování konfigurace

- cronjob, každých 5 minut
- kontrola nových zdrojových dat (LDAP) pomocí modifyTimestamp
- jednou denně force konfigurace
- activity log, diffy konfigurace

Monday, 17th September 2018

[cli] modify user "Vaclav Mach"	13:40:08
[cli] create host "railius2.eduroam.cz"	10:40:08
[cli] modify user "Vaclav Mach"	10:40:08
[cli] modify user "Jan Tomasek"	10:40:08
[cli] create usergroup "railius2.eduroam.cz"	10:40:08

```
1 object User "Vaclav Mach" {
2    email = "Vaclav.Mach@cesnet.cz"
3    groups = [
4         "radius1.cesnet.cz",
5         "radius2.cesnet.cz",
6         "radsec.eduroom.cesnet.cz"
7    ]
8 }
```

```
1 object User "Vaclav Mach" {
2    email = "Vaclav.Mach@cesnet.cz"
3    groups = [
4         "radius1.cesnet.cz",
5         "radius2.cesnet.cz",
6         "radsec.eduroom.cesnet.cz",
7         "railius2.eduroam.cz"
8    ]
9 }
```

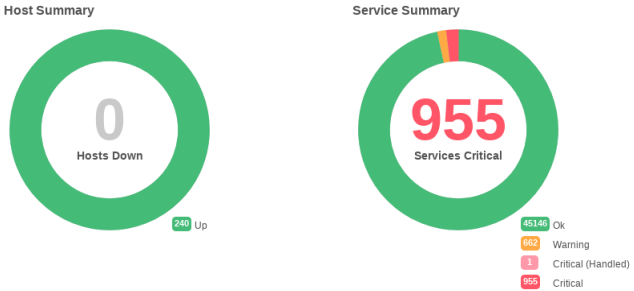
Testy

- závislé na typu realmu (IdPSP, SP, IdP) a typu serveru (infrastrukturní, monitorovaný)
- povinné (notifikované), nepovinné (nenotifikované)
- rad_eap_test – wrapper pro eapol_test
- kompletní přehled na `https://github.com/CESNET/eduroam-icinga/blob/master/doc/tests.md`

cesnet

Testy

- závislé na typu realmu (IdPSP, SP, IdP) a typu serveru (infrastrukturní, monitorovaný)
- povinné (notifikované), nepovinné (nenotifikované)
- rad_eap_test – wrapper pro eapol_test
- kompletní přehled na `https://github.com/CESNET/eduroam-icinga/blob/master/doc/tests.md`



Monitoring eduroamu

Monitoring eduroamu

- dostupnost služby ověřujeme pomocí testovacích účtů všech organizací
- testujeme každého s každým – matice dostupnosti

Matice dostupnosti

- v řádcích jsou servery organizací
- ve sloupcích jsou organizace
- políčko na řádku **a** a ve sloupci **b**: jak funguje eduroam lidem z **b**, pokud jsou na návštěvě v organizaci **a**
- aktuálně testujeme ~ 240 serverů, ~ 220 organizací a více než 45000 služeb

Matice dostupnosti

- zdrojem dat je api icingy (icingacli)

```
{ echo "host_name,service_description,service_state,service_state_type,service_last_check" ;
icingacli monitoring list services --service="*@*"
--format='$host_name$,$service_description$,$service_state$,$service_state_type$,$service_last_check$' \
--columns=host_name,service_state,service_description,service_last_check,service_state_type \
| sortcsvradius.py ; } | jq -R -s -f filter.jq -c -r > data.json
```

- cronjob aktualizuje data každé 2 minuty
- frontend v d3.js
- živě na `https://monitor.eduroam.cz/matrix`
- video na `https://youtu.be/R-8_SS2_XYY`

cesnet

etlog

- systém pro analýzu logů národního RADIUS serveru
- detekuje pravděpodobně kompromitované identity a rychlé přesuny uživatelů
- tato data čerpá monitoring
- vymýšlíme další metody detekce problémů

Uživatelské jméno:	Datum:	1. autentizace:			2. autentizace:			Vzdálenost:	Čas: [hh:mm]		
		Čas:	Instituce:	MAC adresa:	Čas:	Instituce:	MAC adresa:		Teoretický:	Dosažený:	Rozdíl:
[redacted]@vse.cz	26.09.2018	14:41	zcu.cz	[redacted]	14:59	osu.cz	[redacted]	351 km	03:30	00:18	03:12
[redacted]@vse.cz	26.09.2018	17:05	osu.cz	[redacted]	17:26	zcu.cz	[redacted]	351 km	03:30	00:21	03:09
[redacted]@vse.cz	26.09.2018	17:05	osu.cz	[redacted]	17:28	zcu.cz	[redacted]	351 km	03:30	00:22	03:07
[redacted]@vsb.cz	27.09.2018	19:23	ujep.cz	[redacted]	19:24	osu.cz	[redacted]	315 km	03:08	00:01	03:07
[redacted]@vsb.cz	07.09.2018	10:32	osu.cz	[redacted]	10:33	ujep.cz	[redacted]	315 km	03:08	00:01	03:07

cesnet

Problémy monitoringu

- Icinga 2
  - #6629 (otevřený) - příliš časté spouštění testů
- Icinga Director
  - #1455 (vyřešený) - není možné obnovit některé smazané objekty
  - #1462 (zavřený) - není možné mazat více objektů najednou
  - #1636 (otevřený) - nesprávně fungující filtry v importních zdrojích
- Monitoring Plugins
  - #6629 (otevřený) - plugin ping4 komunikuje po IPv6

cesnet

Icinga Web 2

Jako webové rozhraní používáme Icinga Web 2.

- problémy s utf-8
- rychlost odezvy webu

cesnet

Dokumentace, zdrojové kódy

Vše veřejně na githubu

- setup monitoringu - `https://github.com/CESNET/eduroam-icinga`
  - dokumentace pro nás
  - snaha o dokumentaci monitoringu jako celku tak, aby mohl znovupoužít kdokoliv
- podpůrné nástroje (matice) - `https://github.com/CESNET/eduroam-monitor`
- etlog - `https://github.com/CESNET/etlog`
- rad_eap_test - `https://github.com/CESNET/rad_eap_test`

cesnet

Dotazy

Dotazy?

připomínky na
vaclav.mach@cesnet.cz

cesnet