

C2110 Operační systém UNIX a základy programování

2. lekce / modul 1

PS/2021 Prezenční forma výuky: Rev3

Petr Kulhánek

kulhanek@chemi.muni.cz

Národní centrum pro výzkum biomolekul, Přírodovědecká fakulta
Masarykova univerzita, Kamenice 5, CZ-62500 Brno

Kerberos

https://cs.wikipedia.org/wiki/Kerberos_%28protokol%29

Aneb proč to po mne pak nechce heslo?

Podrobnější informace v kurzu C2115.

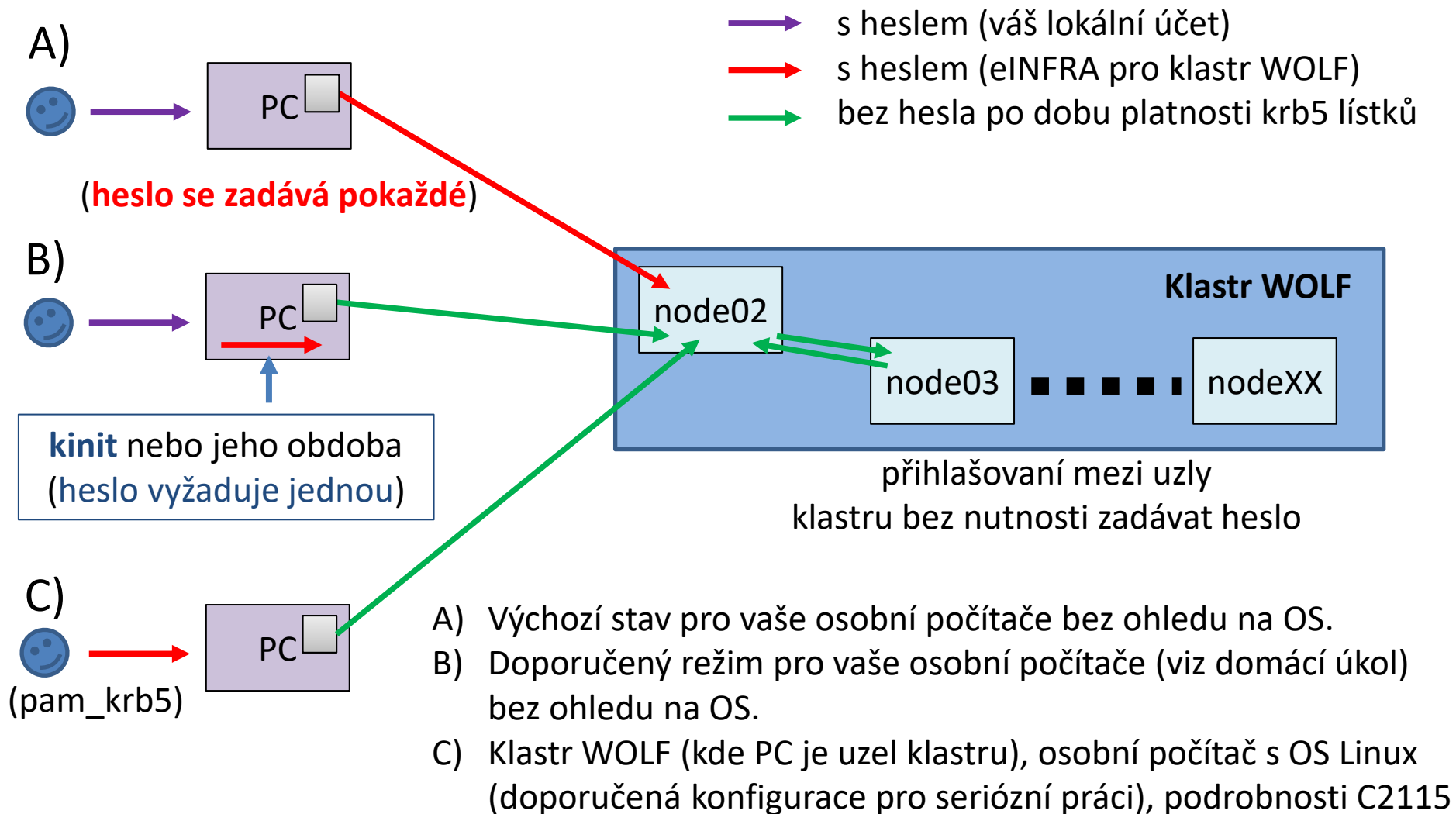
Kerberos

Na klastru WOLF je využíván **system Kerberos** k ověřování identity uživatele. Po primárním ověření (přihlašovací jméno/heslo), uživatel získá lístek z realmu **META**, který jej opravňuje bez opětovného zadávání hesla využívat služby klastru či se přihlašovat na jiné klastry využívající k autentizaci stejný realm (např. MetaCentrum) a to po celou dobu platnosti lístku.

Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou autentizaci – klient i server si ověří identitu své protistrany. Kerberos je postavený na symetrické kryptografii, a proto potřebuje důvěryhodnou třetí stranu. Volitelně může využívat asymetrického šifrování v určitých částech autentizačního procesu.

Kerberos má **přísné požadavky na synchronizaci času klientů a serverů**. Tikety mají danou životnost a pokud není čas klienta synchronizován s časem serveru, autentizace selže. Standardní nastavení podle MIT požaduje, aby se tyto časy **nerozcházely o více jak 5 minut**. V praxi se používá **NTP (Network Time Protocol)** démonů k synchronizaci hodin.

Workflow



!!! V prostředí, které využívá krb autentizaci, se NEDOPORUČUJE používat ssh klíče !!!

Vypršení lístků

Pokud vyprší lístek, tak bude odmítnut další přístup ke službám, které jej vyžadují. To může vést k viditelným chybám s odepřením přístupu. **Některé chyby se však viditelně neprojeví a hledání příčiny tak nemusí být "snadné"**. Typicky tato situace nastává u sezení, které jsou otevřené déle než je platnost kerberovského lístku a týká se převážně software aktivovaného pomocí příkazu module a fyzicky umístěného na AFS souborovém systému (téměř většina software v MetaCentru a na klastru WOLF).

Pokud se něco začne chovat divně (nefungující softwarové moduly), tak si nejdříve ověřte, že máte platné kerberovské lístky (klist) a případně je znovu vytvořte (kinit).

Příkazy

- kinit** vytvoří nový kerberovský lístek
- klist** vypíše existující kerberovské lístky
- kdestroy** odstraní existující kerberovské lístky

Na klastru WOLF se kerberovské lístky vytváří při prvotním přihlášení a obnovují při každém odemčení sezení.

```
[kulhanek@pes ~]$ kinit
Password for kulhanek@META:
[kulhanek@pes ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: kulhanek@META
```

realm pro META



```
Valid starting          Expires                Service principal
01/30/2016 23:28:30    01/31/2016 23:28:24  krbtgt/META@META
[kulhanek@pes ~]$ kdestroy
[kulhanek@pes ~]$ klist
klist: No credentials cache found (ticket cache
FILE:/tmp/krb5cc_1001)
[kulhanek@pes ~]$
```

Cvičení 1

1. (Distančně) Přihlaste se na pracovní stanici wolf03.ncbr.muni.cz (ssh, putty, apod.).
2. Získali jste kerberovské lístky? Ověřte jejich stav (**klist**). Kdy vyprší?
3. Z aktuálního terminálu se přihlaste na stroj wolf06 příkazem ssh. Je vyžadováno heslo?
4. Získali jste kerberovské lístky? Ověřte jejich stav (**klist**). Kdy vyprší?
5. Odhlaste se ze stroje wolf06 (exit).
6. Akci opakujte (body 3, 4, 5), ale lístky nejdříve odstraňte příkazem **kdestroy**.
7. Akci opakujte (body 3, 4, 5), ale lístky nejdříve obnovte příkazem **kinit**.
8. Pokud máte účet v MetaCentru, přihlaste se na stroj skirit.ics.muni.cz ze stroje wolf03. Je vyžadováno heslo?

Domácí úkoly



Domácí úkol

1. Na vašem osobním počítači si zprovozněte variantu B workflow ze strany 4. Postup naleznete v doprovodné prezentaci podle typu OS vašeho počítače.