C2110 *Operační systém UNIX a základy programování*

U04: Kerberos

PS/2022 Prezenční forma výuky: Rev5

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

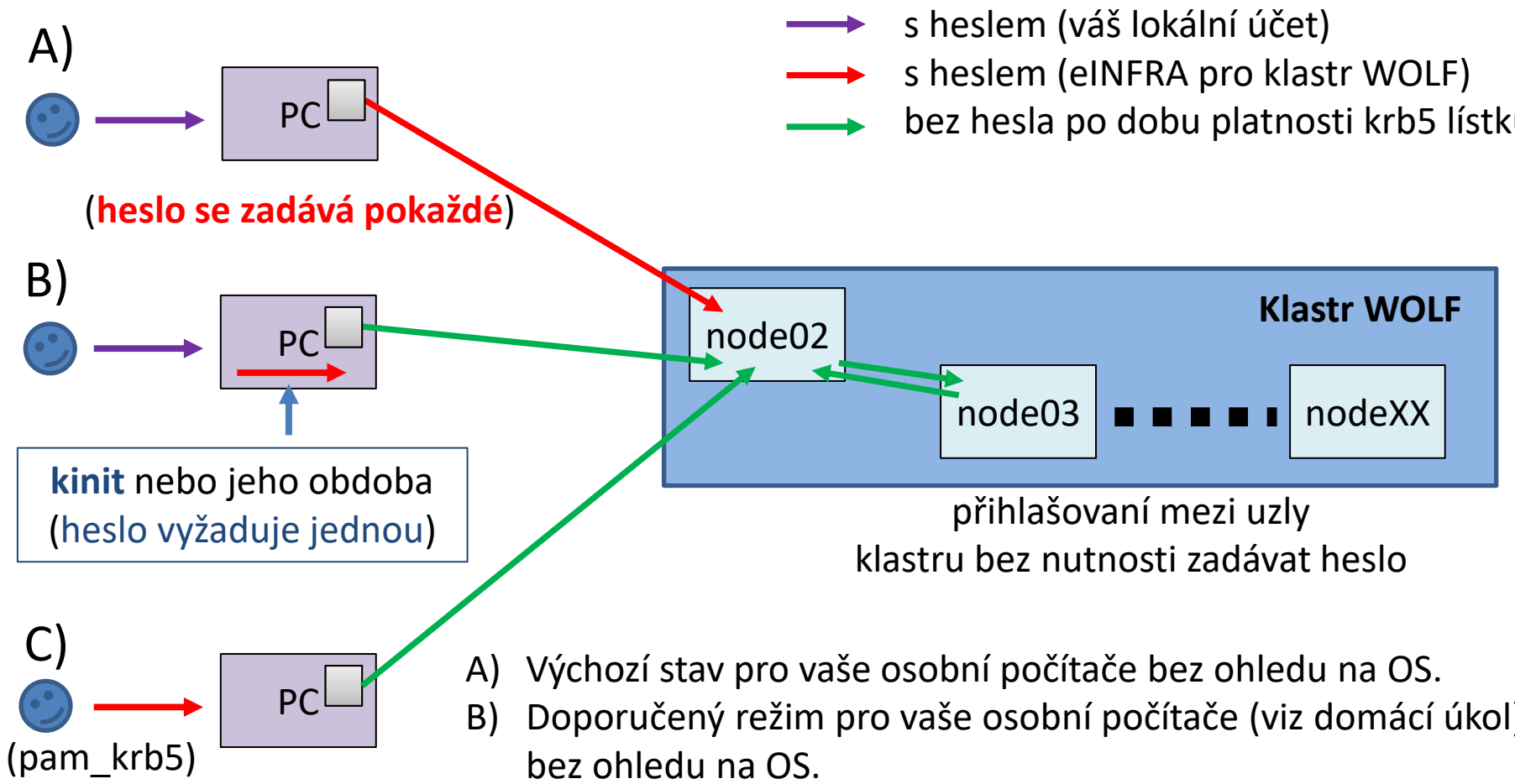
Na klastru WOLF je využíván **systém Kerberos** k ověřovaní identity uživatele. Po primárním ověření (přihlašovací jméno/heslo), uživatel získá lístek z realmu **META**, který jej opravňuje bez opětovného zadávání hesla využívat služby klastru či se přihlašovat na jiné klastry využívající k autentizaci 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.

wikipedia.org

Workflow



A) Výchozí stav pro vaše osobní počítače bez ohledu na OS.
B) Doporučený režim pro vaše osobní počítače (viz domácí úkol) bez ohledu na OS.
C) Klastr WOLF (kde PC je uzel klastru), osobní počítač s OS Linux (doporučená konfigurace pro seriózní práci), podrobnosti C2115

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

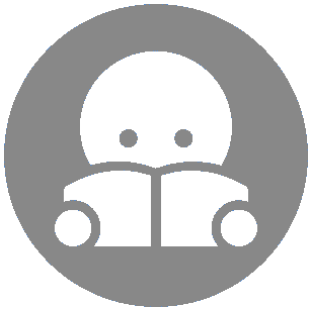
realm pro META

zápis hesla se neindikuje (žádné tečky, hvězdičky)

Cvičení 1

1. Otevřete nový terminál.
2. Ověřte stav lístků příkazem **klist**. Kdy byly vystaveny a kdy vyprší?
3. Lístky odstraňte příkazem **kdestroy**.
4. Ověřte stav lístků (**klist**).
5. Přihlaste se na stroj wolf01 příkazem **ssh**. Je vyžadováno heslo?
6. Máte po přihlášení na stroj wolf01 lístky? Kdy byly vystaveny?
7. Odhlaste se ze stroje wolf01 příkazem **exit**.
8. Ověřte stav lístků (**klist**).
9. Obnovte lístky příkazem **kinit**.
10. Ověřte stav lístků (**klist**).
11. Přihlaste se na stroj wolf01 příkazem **ssh**. Je vyžadováno heslo?
12. Máte po přihlášení na stroj wolf01 lístky? Kdy byly vystaveny a do kdy platí?
13. Odhlaste se ze stroje wolf01.

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.