Revize 5

C2115 Praktický úvod do superpočítání

5. lekce / Modul 2

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

Kerberos

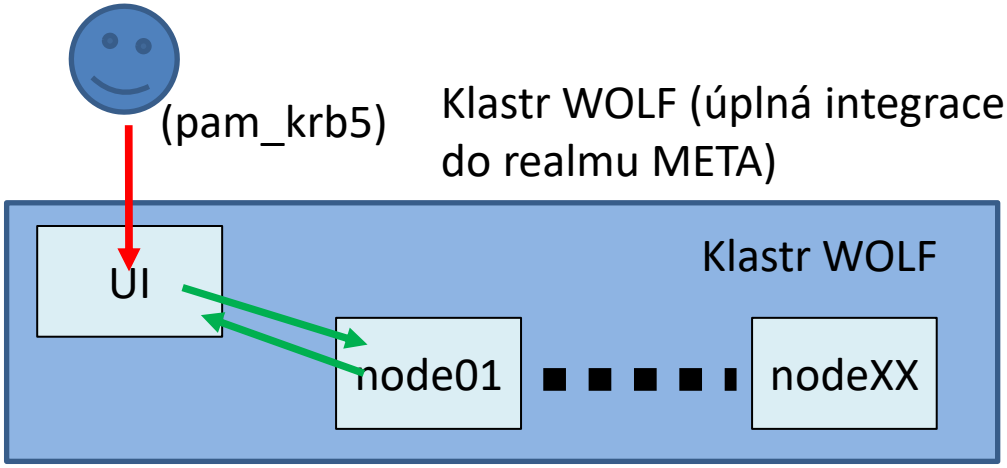
Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou 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.

Na klastru WOLF jsou při přihlášení vytvořené krb5 lístky z realmu META, které je možné použít pro autentizaci za účelem přihlášení se na čelní uzly MetaCentra, pro kopírování dat příkazem scp z/do čelních uzlů a pro připojení datových úložišť MetaCentra na klastr WOLF.

wikipedia.org

Workflow - místní přihlášení

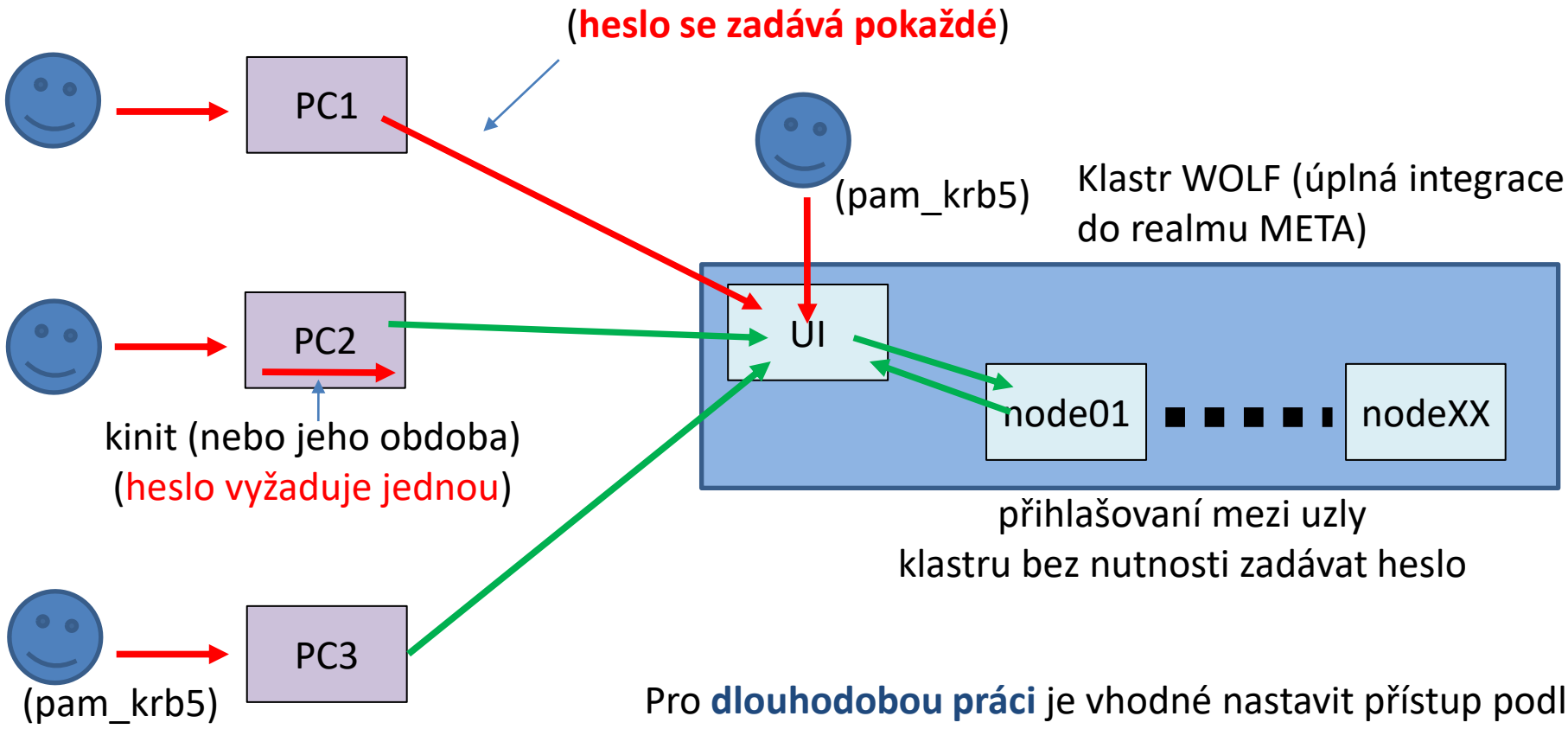


přihlašovaní mezi uzly klastru bez nutnosti zadávat heslo

s heslem

bez hesla po dobu platnosti krb5 lístků

Workflow - vzdálené přihlášení



Pro **dlouhodobou práci** je vhodné nastavit přístup podle varianty **PC2** (MS Windows, Linux, macOS) nebo PC3 (pouze linux).

s heslem

bez hesla po dobu platnosti krb5 lístků

Příkazy

kinit	vytvoří nový krb5 lístek
klist	vypíše existující krb5 lístky
kdestroy	odstraní existující krb5 lístky

realm pro MetaCentrum

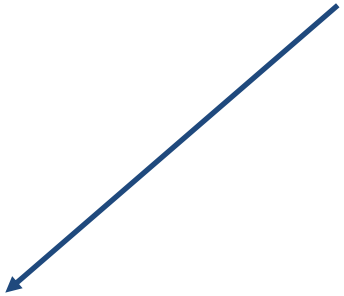
```
[kulhanek@pes ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: kulhanek@META

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 credentials cache found (ticket cache
FILE:/tmp/krb5cc_1001)
[kulhanek@pes ~]$ kinit
Password for kulhanek@META:
[kulhanek@pes ~]$ klist
```

zadávaní hesla se neindikuje

kinit

Příkaz **kinit** slouží k vytvoření/obnově krb5 lístků.



jméno principálu se odvozuje od principálu v cachi kerborovských lístků, pokud tento soubor neexistuje, tak od **přihlašovacího jména a výchozího realmu** (META)

```
$ kinit
```

```
$ kinit kulhanek
```

zadané jméno plus výchozí realm (META)

```
$ kinit kulhanek@META
```

použije se zadaný principál

Pokud používáte na lokálním stroji jiné přihlašovací jméno než v eINFRA prostoru (realm META), tak jej musíte explicitně uvést jako argument příkazu **kinit**.

Na klastru WOLF získáte krb5 lístky automaticky při přihlášení. Příkaz kinit se tedy používá pouze při obnově vypršených lístků.

ssh a kerberos

ssh je možné nastavit tak, aby se uživatel ověřoval pomocí krb5 lístků (GSSAPIAuthentication) a aby se krb5 lístky přenášely na vzdálený stroj (GSSAPIDelegateCredentials). Toto je výchozím nastavením klastrů NCBR, CEITEC MU a MetaCentra.

```
[kulhanek@wolf ~]$ kinit
Password for kulhanek@META:
[kulhanek@wolf ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_9703
Default principal: kulhanek@META
Valid starting       Expires              Service principal
02/02/2016 08:13:53  02/03/2016 08:13:49  krbtgt/META@META
[kulhanek@wolf ~]$ ssh kulhanek@skirit.ics.muni.cz
...
...
[kulhanek@skirit ~]$
[kulhanek@skirit ~]$ klist
Credentials cache: FILE:/tmp/krb5cc_18773_GcLXWPTirK
        Principal: kulhanek@META
  Issued                Expires               Principal
Feb  2 08:14:18 2016  Feb  3 08:13:49 2016  krbtgt/META@META
....
```

neopakuje se v době platnosti lístků

uvádí se pouze tehdy, pokud máte jiné přihlašovací jméno

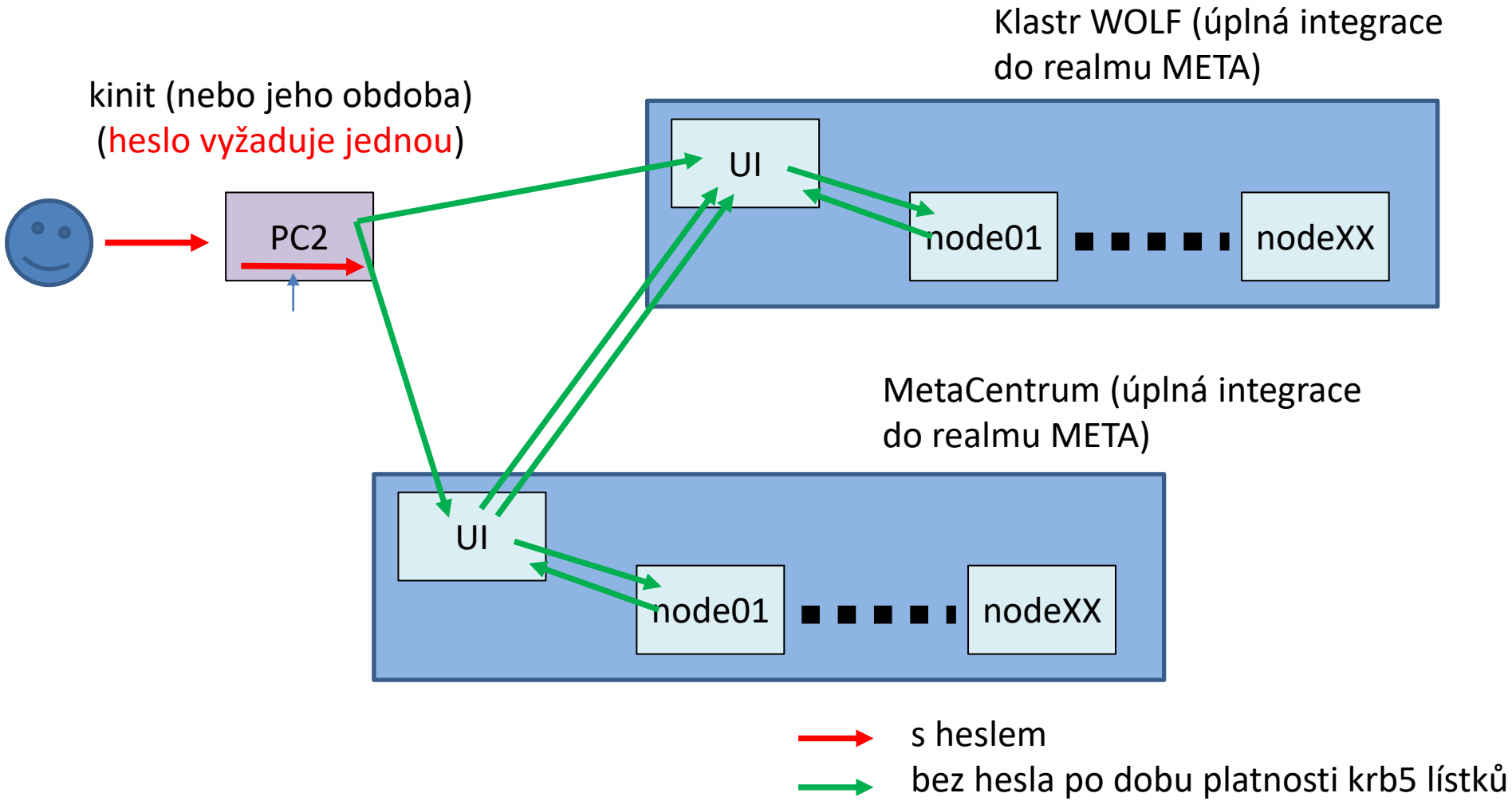
nevyžaduje heslo

Cvičení M2.C1

1. Ověřte, že máte platné krb5 lístky. Jakou mají platnost?
2. Příkazem ssh se přihlaste na libovolný čelní uzel MetaCentra (příkaz ssh nesmí žádat heslo).
3. Na čelním uzlu ověřte, že se kerberovské lístky správně přenesly. Jakou mají platnost?
4. Odhlaste se.
5. Zrušte lístky příkazem kdestroy.
6. Znovu se pokuste přihlásit na libovolný čelní uzel MetaCentra, co pozorujete?
7. Jakou platnost mají vytvořené kerberovské lístky na čelním uzlu?
8. Můžete se přihlásit z čelního uzlu MetaCentra na vaši pracovní stanici na klastru WOLF?

Workflow - vzdálené přihlášení

Vzdálené přihlášení mezi klastry ve stejném krb5 realmu



Platnost lístků/Obnovitelné lístky

Platnost lístků je časově omezena, typicky několik hodin. To je nepraktické při spouštění dlouhodobých úloh. Pro tyto účely je možné **vytvořit obnovitelné lístky (renewable tickets)**. Jejich platnost je opět časově omezena, ale v době jejich platnosti je možné požádat (bez uvedení hesla) o jejich obnovu. Tento proces je možné opakovat po delší dobu, typicky několik dní.

Na našich klastrech a MetaCentru se kerberovské lístky v úlohách spuštěných přes dávkový systém obnovují automaticky.

Příklad:

```
[kulhanek@pes ~]$ kinit -r 5d
Password for kulhanek@META:
[kulhanek@pes ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: kulhanek@META

Valid starting       Expires              Service principal
01/31/2016 10:42:22  02/01/2016 10:42:18  krbtgt/META@META
        renew until 02/05/2016 10:42:1
[kulhanek@pes ~]$ kinit -R
```

obnoví lístek (volba velké R), je možné jenom v době platnosti stávajícího lístku

Umístění lístků (cache)

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

Valid starting       Expires              Service principal
01/31/2016 11:23:55  02/01/2016 11:23:52  krbtgt/META@META

[kulhanek@pes ~]$ ssh onyx.ncbr.muni.cz
...
...
[kulhanek@onyx ~]$ klist
Credentials cache: FILE:/tmp/krb5cc_18773_cOR8E0oV8w
        Principal: kulhanek@META

  Issued                Expires               Principal
Jan 31 11:25:48 2016  Feb  1 11:23:52 2016  krbtgt/META@META
...
```

generické jméno odvozené od uid, dostupné ve všech terminálech (podle konfigurace OS může obsahovat i náhodný řetězec)

cache nastavená pouze pro dané sezení **(náhodný řetězec)**

Cache s lístky nesmí být umístěna na sdíleném svazku (NFS apod).

Vypršení lístků

Jakmile vyprší lístek, 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 (softwarová báze MetaCentra a Infinity).

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).

AFS souborový systém

Softwarová báze MetaCentra a prostředí Infinity je umístěná na AFS souborovém systému. (adresáře /afs/ics.muni.cz/software a /afs/ics.muni.cz/software/ncbr). Tento FS využívá pro řízení přístupu k souborům a adresářům autentizační tokeny odvozené z krb5 lístků.

Příkazy:

tokens	vypíše AFS tokeny
aklog	vytvoří AFS tokeny (z platných krb5 lístků), popř. je možné požít příkaz **afslog**
unlog	odstraní AFS tokeny

Implementace Kerbera

MIT Kerberos

- kinit **neobnovuje** AFS tokeny

(Ubuntu balíček: krb5-user)

Heimdal Keberos

- kinit **obnovuje** AFS tokeny

(Ubuntu balíček: heimdal-clients*)

* výchozí balíček v MetaCentru a našich klastrech

Cvičení M2.C2

1. Na klastru WOLF vypište AFS tokeny. Pro jaké AFS buňky jsou vydané?
2. Co je to AFS buňka?
3. Změňte adresář do /afs/ics.muni.cz/software/ncbr/softrepo/ncbr
4. Vraťte se do domovského adresáře.
5. Odstraňte AFS tokeny.
6. Změňte adresář do /afs/ics.muni.cz/software/ncbr/softrepo/ncbr. Co se stane?
7. Obnovte AFS tokeny.
8. Přihlaste se na čelní uzel MetaCentra. Pro jaké AFS buňky máte vytvořené AFS tokeny?