C2115
Praktický úvod do superpočítání

VII. lekce

Petr Kulhánek

kulhanek@chemi.muni.cz

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

Obsah

- **Autentizace**
  - **Autentizace vs Authorizace**
  - **Sekundární autentizace v superpočítačových centrech**
    - **Kerberos**
    - **SSH klíče**
  - **Konfigurace, balíčky**

Autentizace vs Autorizace

Autentizace (z německého Authentisierung) je proces ověření proklamované identity subjektu. Po dokončení autentizace obvykle následuje autorizace, což je souhlas, schválení, umožnění přístupu či provedení konkrétní operace daným subjektem.

Autorizace je proces získávání souhlasu s provedením nějaké operace, povolení přístupu někam, k někomu nebo něčemu (nejen ve smyslu přístupu do konkrétních prostor nebo k nějaké osobě, ale také přístup k informacím, funkcím, programovým objektům a podobně).

Nejčastějším způsobem **primární autentizace** je kombinace přihlašovacího jména a hesla (lokální klastry, WOLF, MetaCentrum). V IT4I je primární autentizace umožněna pouze pomocí ssh klíčů.

Superpočítače se většinou skládají z velkého množství výpočetních uzlu a bylo by velmi nepraktické či nemožné (např. při dávkovém spouštění úloh) se prokazovat heslem při každém přihlašování na výpočetní uzel. Při **sekundární autentizaci** se proto používá jiná technika.

wikipedia.org

Sekundární autentizace

Primární autentizace vytvoří stav, který se později využije k autentizaci (sekundární autentizace) bez nutnosti znovu zadávat heslo. Tento stav může nebo nemusí být časově omezen. Nejčastěji se používají Kerberos nebo ssh klíče.

Naše lokální klastry (WOLF, sokar, pip, ivavik) a MetaCentrum:

- e-infrastrukturu CESNETu (autentizace a autorizace řízená Perunem)
- Kerberos (realm META)
- Správa uživatelských účtů je zajišťována Perunem (instance CESNETu)

https://perun.cesnet.cz

Superpočítačové centrum IT4I:

- ssh klíče

Cvičení 1

1. Přihlaste se do prostředí Perun.
2. Prakticky: Perun z pohledu uživatele a správce.
3. Kde mohu změnit heslo k eINFRA účtu?

Kerberos

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

Kerberos

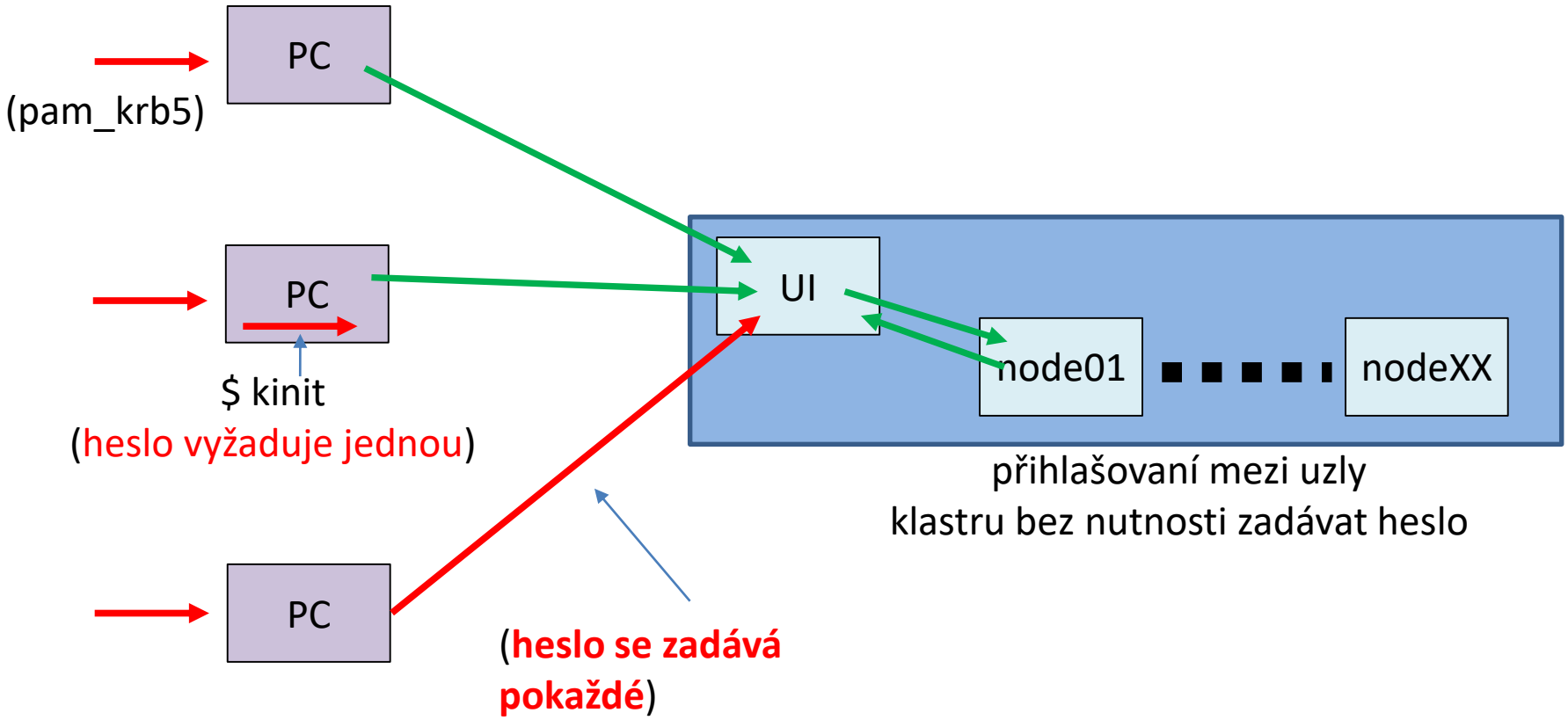
Kerberos je síťový autentizační protokol umožňující komukoli komunikujícímu v nezabezpečené síti prokázat bezpečně svoji identitu někomu dalšímu. Kerberos zabraňuje odposlechnutí nebo zopakování takovéto komunikace a zaručuje integritu dat. Byl vytvořen primárně pro model klient-server a poskytuje vzájemnou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



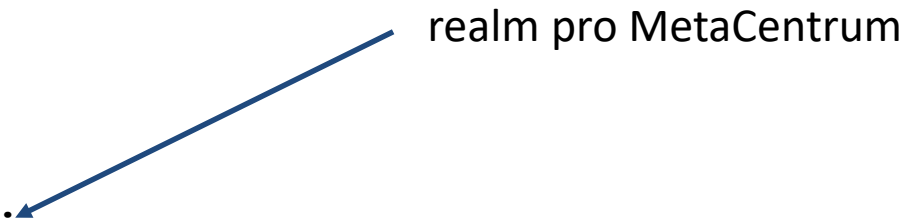
Klastr WOLF se chová dle první varianty.

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




```
[kulhanek@pes ~]$ kinit
Password for kulhanek@META:
[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

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

```
$ kinit
```

zadané jméno plus výchozího realm (META)

```
$ kinit kulhanek
```

použije se zadaný principál

```
$ kinit kulhanek@META
```

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

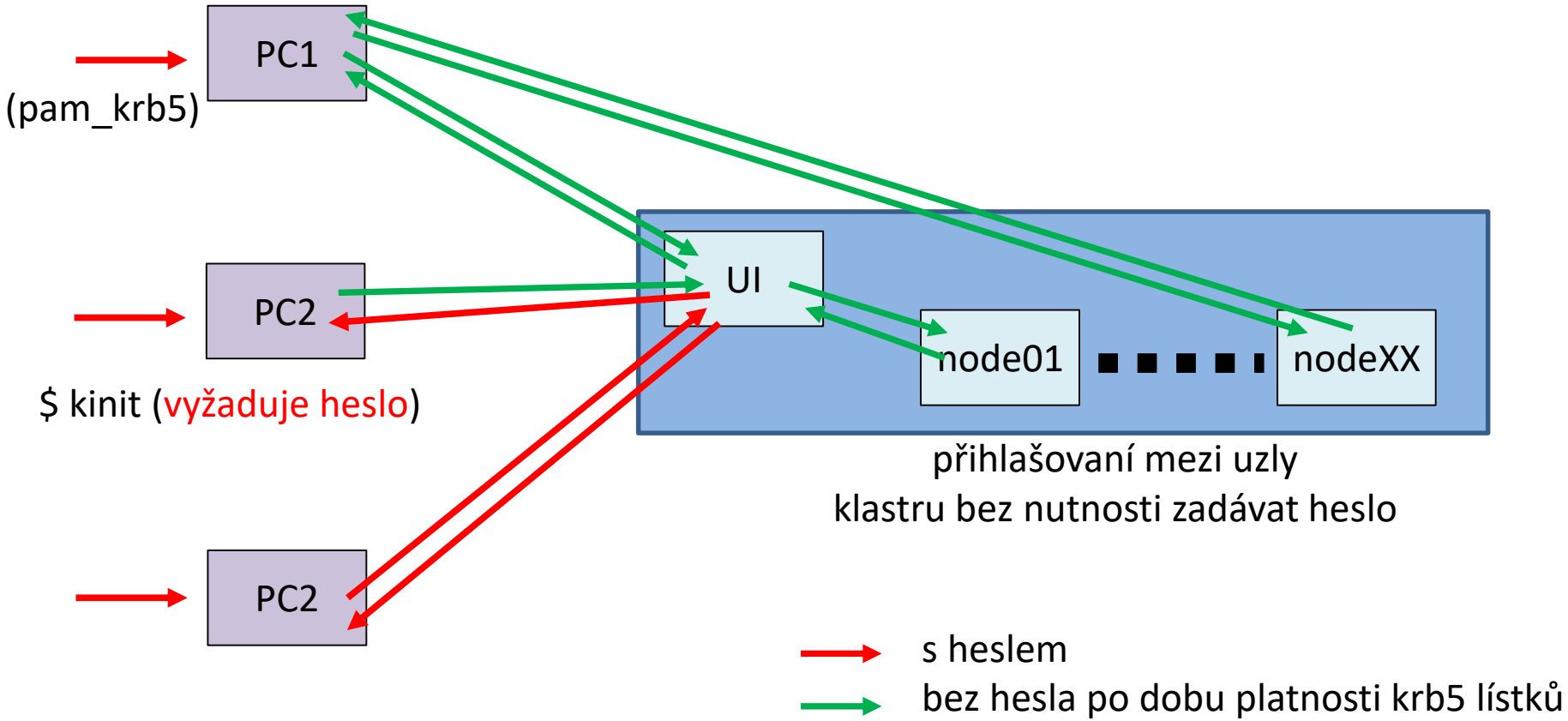
Cvičení 2

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

PC1 (např. pracovní stanice klastru WOLF) je ve stejném krb5 realmu jako klastr.

PC2 je nezávislý počítač.



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

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 (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)
unlog	odstraní AFS tokeny

Implementace Kerbera

MIT Kerberos

- kinit **neobnovuje** AFS tokeny

(Ubuntu balíček: krb5-user)

Heimdal Keberos

- kinit **obnovuje** AFS tokeny

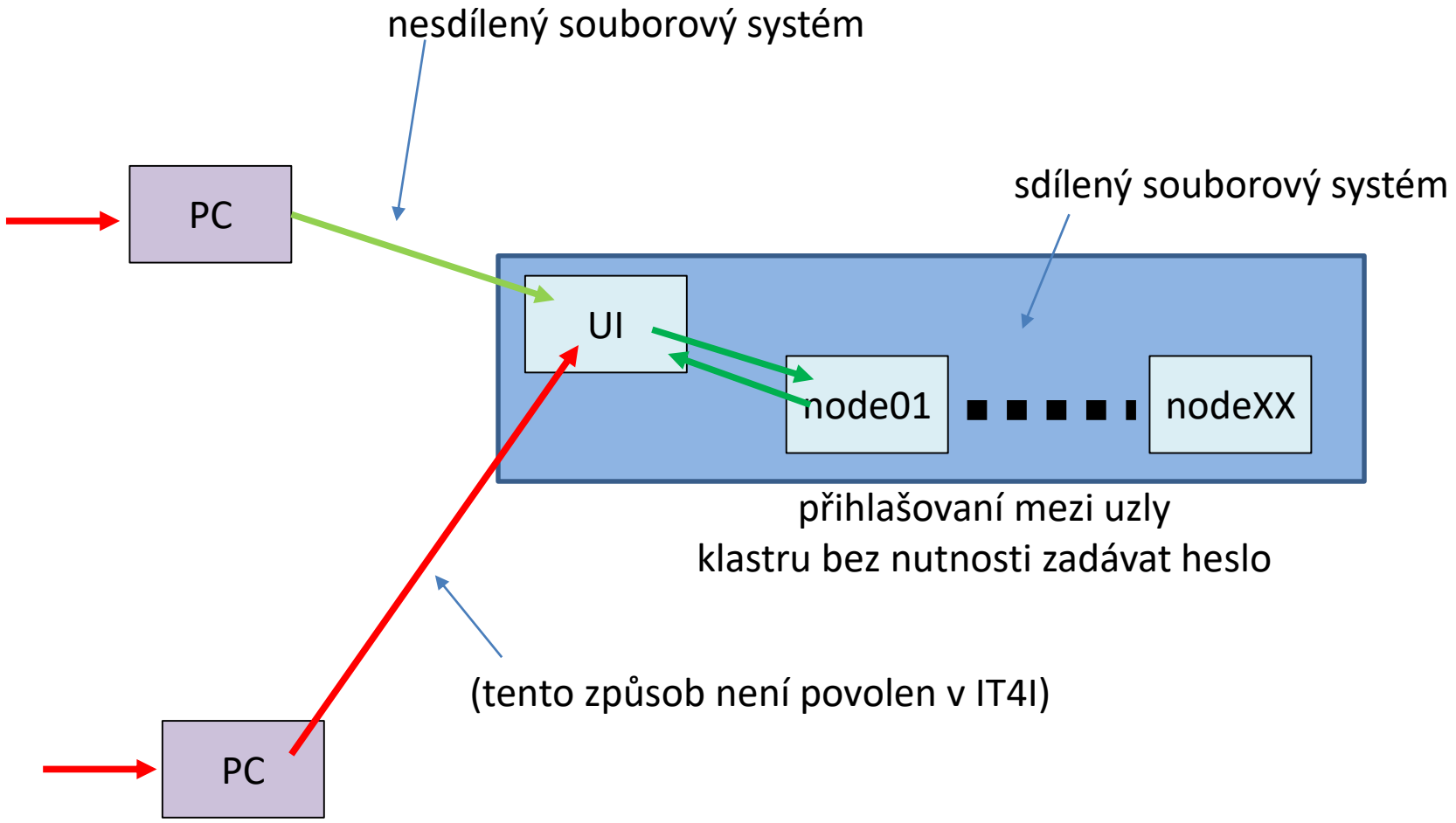
(Ubuntu balíček: heimdal-clients*)

* výchozí balíček v MetaCentru a našich klastrech

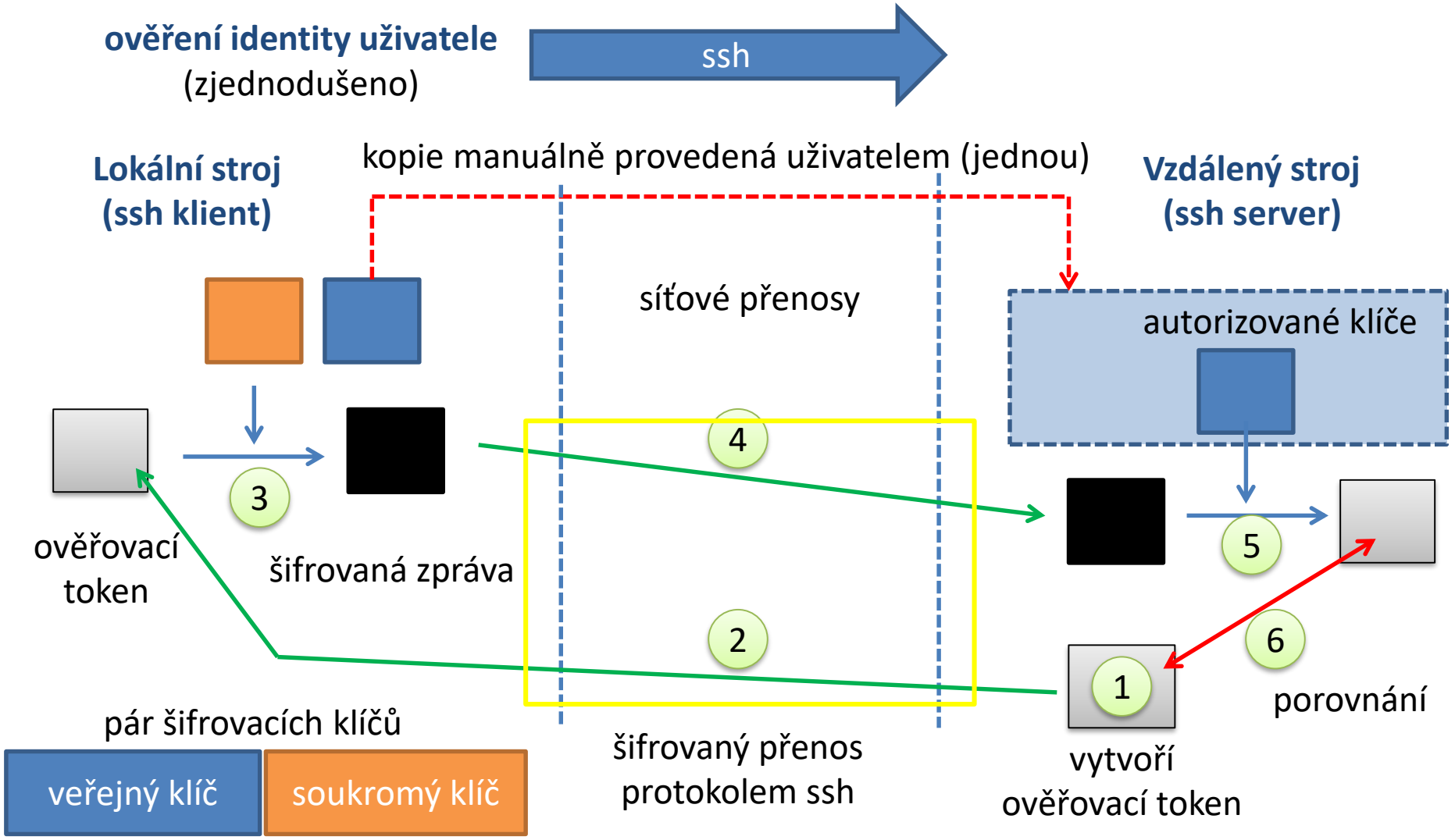
SSH klíče

man ssh

Workflow


nesdílený souborový systém
PC
sdílený souborový systém
UI
node01
nodeXX
přihlašovaní mezi uzly
klastru bez nutnosti zadávat heslo
(tento způsob není povolen v IT4I)
PC
s heslem
bez hesla s ssh klíčem #1
bez hesla s ssh klíčem #2

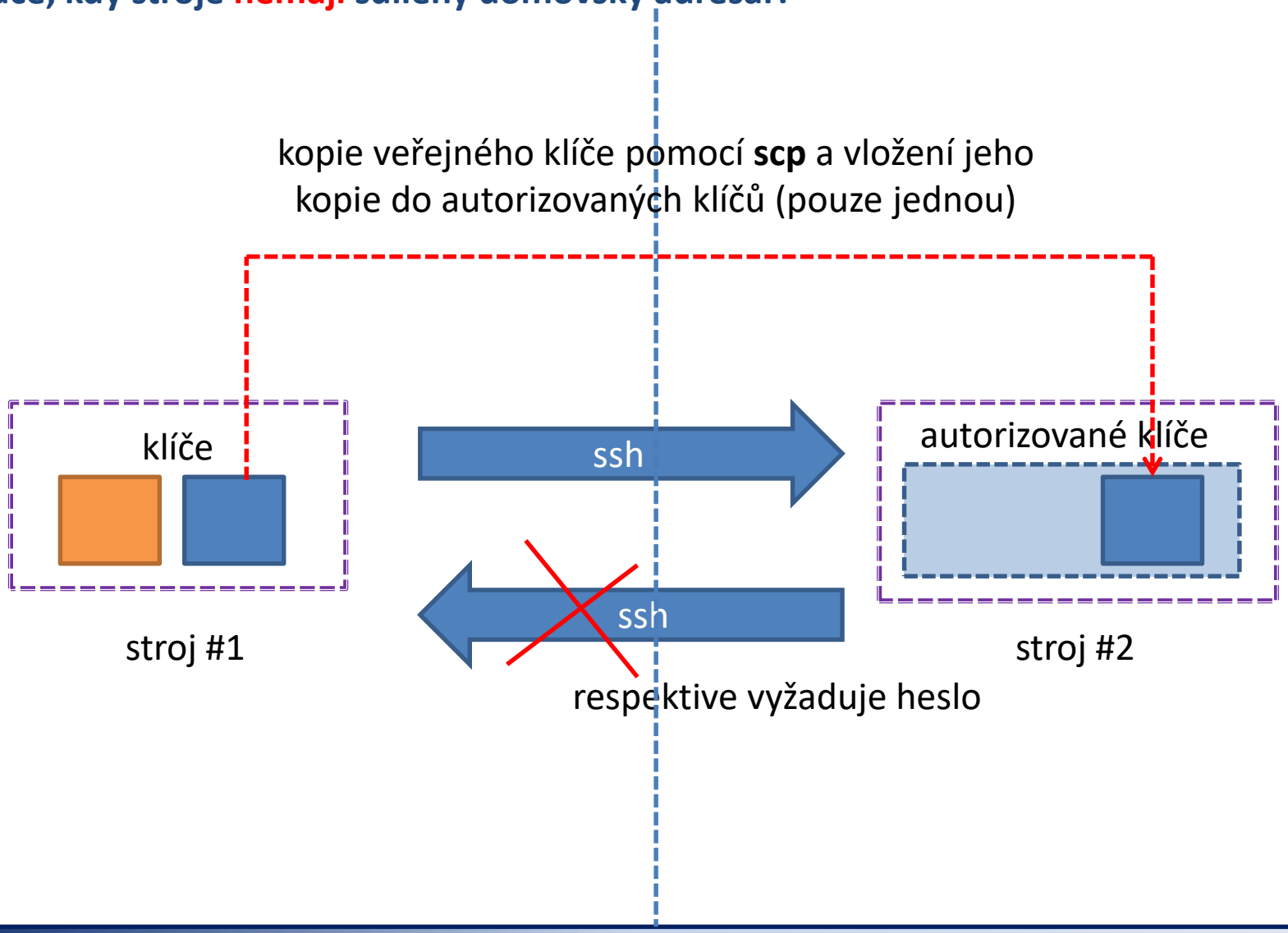
Autorizovaný veřejný ssh klíč



Kdokoliv, kdo zcizí soukromý klíč uživatele, se může přihlásit na vzdálený stroj!

Nesdílený souborový systém

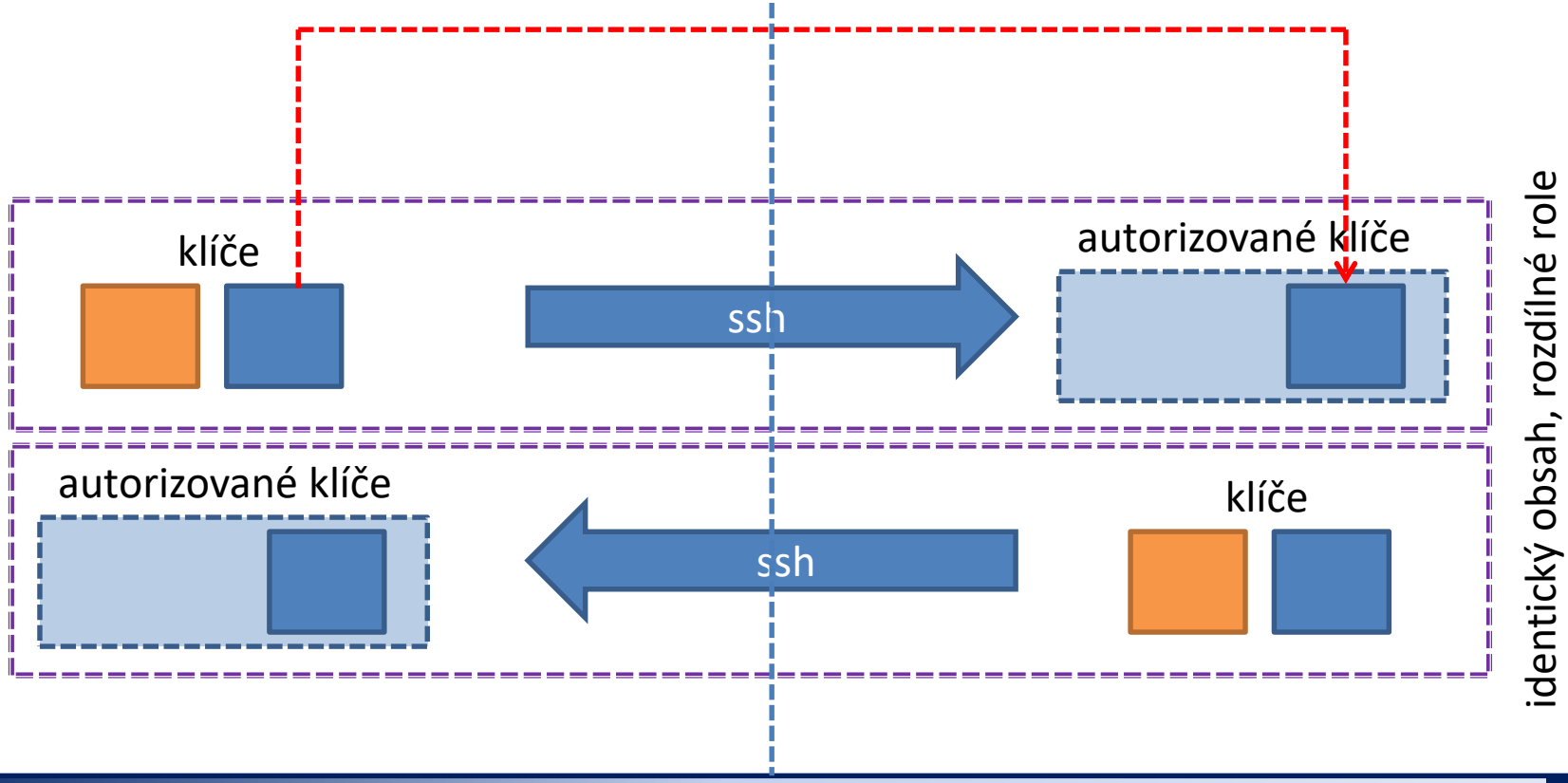
Situace, kdy stroje nemají sdílený domovský adresář:



Sdílený souborový systém

Situace, kdy stroje mají sdílený domovský adresář:

oba soubory jsou na sdíleném souborovém systému
je možné použít (pouze jednou)
cat id_rsa.pub >> authorized_kyes



Vytvoření páru v/s klíče

Pár veřejného a soukromého klíče se vytváří na daném stroji nebo skupině strojů, které mají sdílený adresář, POUZE jednou.

```
[kulhanek@wolf01 ~]$ cd .ssh

[kulhanek@wolf01 .ssh]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kulhanek/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/kulhanek/.ssh/id_rsa.
Your public key has been saved in /home/kulhanek/.ssh/id_rsa.pub.
The key fingerprint is:
e9:07:0b:fc:17:23:b3:c5:1a:8a:0c:1a:98:8f:fe:28 kulhanek@wolf01.wolf.inet

[kulhanek@wolf01 .ssh]$ ls -l
-rw------- 1 kulhanek lcc  1675 Mar 21  2012 id_rsa
-rw-r--r-- 1 kulhanek lcc   395 Mar 21  2012 id_rsa.pub
-rw------- 1 kulhanek lcc 13380 Sep  4 15:55 known_hosts
```

Passphrase se nezadává!

soukromý klíč NESMÍ být čitelný pro skupinu a svět

seznam otisků palců strojů, na které jste se přihlásili pomocí příkazu ssh

Podrobnější popis: man ssh

Vytvoření autorizovaných klíčů - I

sdílený souborový systém

Vložení veřejného klíče do seznamu autorizovaných klíčů:

```
[kulhanek@node ~]$ cd .ssh
[kulhanek@node ~]$ cat id_rsa.pub >> .ssh/authorized_keys

[kulhanek@node .ssh]$ ls -l
-rw-r--r-- 1 kulhanek lcc   395 Sep 25  2012 authorized_keys
```

přístupová práva pro soubor authorized_kyes, **pro skupinu a jiné - maximálně právo pro čtení**

Soubor *authorized_keys* může obsahovat více veřejných klíčů, každý je pak na jedné řádce.

Pokud přihlašování pomocí autorizovaných veřejných klíčů nebude fungovat :

- ověřte přístupová práva jednotlivých souborů (písmenka r, w (eventuálně x) ve výpisu příkazu ls)
- pokud běží ssh agent, odstraňte klíče, které má ve správě:

```
$ ssh-add -D
```

- znovu se přihlaste

Podrobnější popis: man ssh

Vytvoření autorizovaných klíčů II

nesdílený souborový systém

Veřejný klíč je nutné překopírovat na vzdálený klastr. Ke vzdálenému kopírovaní slouží příkaz **scp**.

Syntaxe:

[] - možno vynechat

```
$ scp [-r] zdroj cil
```

Zdroj a cíl může být soubor nebo adresář. V případě kopírovaní adresářů je nutno použít volbu **–r** (recursive).

Vzdálený cíl nebo host se identifikuje názvem stroje odděleného od jména souboru či adresáře **dvojtečkou**.

```
[user@]hostname:[cesta/]soubor
```

Vytvoření autorizovaných klíčů II

nesdílený souborový systém

Vložení veřejného klíče do seznamu autorizovaných klíčů :

Získání veřejného klíče ze stroje, který bude mít roli klienta (chceme z něj spouštět příkaz ssh):

```
[kulhanek@ui ~]$ scp wolf.ncbr.muni.cz:.ssh/id_rsa.pub wolf.pub
```

Zapsání veřejného klíče do seznamu autorizovaných klíčů:

dvojtečka tečka

```
[kulhanek@ui ~]$ cat wolf.pub >> .ssh/authorized_keys
[kulhanek@ui ~]$ rm wolf.pub
[kulhanek@ui ~]$ ls -l .ssh
-rw-r--r-- 1 kulhanek lcc   395 Sep 25  2012 authorized_keys
-rw------- 1 kulhanek lcc  1675 Mar 21  2012 id_rsa
-rw-r--r-- 1 kulhanek lcc   395 Mar 21  2012 id_rsa.pub
-rw------- 1 kulhanek lcc 13380 Sep  4 15:55 known_hosts
```

přístupová práva pro soubor authorized_kyes,
pro skupinu a jiné – maximálně jen právo pro čtení

Podrobnější popis: man ssh

Cvičení 3

1. Nastavte vaši instanci virtuálního stroje s Ubuntu tak, abyste se do něj mohli přihlásit pomocí ssh klíčů z hostitelského stroje.
2. Můžete se do virtuálního stroje přihlásit bez hesla ze stroje wolf01? Chování vysvětlete.

Pro a proti

Výhody:

- nemusí se neustále zadávat heslo
- bezpečnější použití příkazů ssh a scp ve skriptech
- urychlení práce

Nevýhody:

- v případě kompromitace jednoho počítače, jsou kompromitovány všechny počítače se vzájemně autorizovanými veřejnými klíči

- **SSH klíče zásadně nepoužívejte pro přihlašovaní do MetaCentra nebo na klastech NCBR či CEITEC MU. Nevytvoří se během něj kerberovské lístky, bez kterých je prostředí těchto klastru nepoužitelné!!!!**

Instalace Kerbera pro realm META

pomocí balíčků pro OS Ubuntu 16.04 LTS

Instalace pomocí balíčků

1) Aktivace **veřejného repositáře NCBR balíčků**.
   Postup je uveden na **https://wolf.ncbr.muni.cz** v části „Uživatelská podpora“ a repositář CEITEC MU/NCBR PUBLIC.
   Repositář se **aktivuje pouze jednou.**

```
https://wolf.ncbr.muni.cz/whitezone/packages/public/16.04/
```

2) Podpora Kerbera pro Metacentrum (konfigurace a heimdal clients):

```
$ sudo apt-get install ncbr-krb5-einfra
```

3) Podpora Kerbera v ssh (GSSAPIAuthentication a GSSAPIDelegateCredentials)

```
$ sudo apt-get install ncbr-ssh-client-config
```

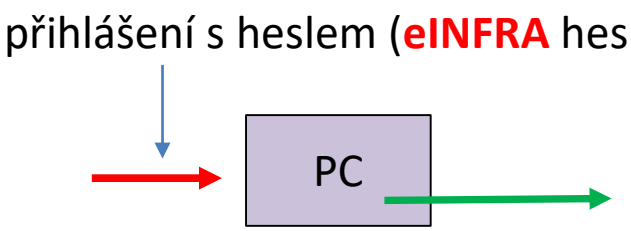
4) Konfigurace pam_krb5 (získání krb5 lístku při prvním přihlášení)

```
$ sudo apt-get install ncbr-personal-authc-einfra
```

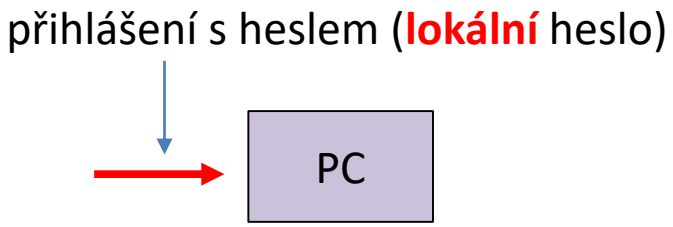
UPOZONĚNÍ: NCBR balíčky jsou autorativní. Konfigurace, kterou balíčky nastavují již není možné měnit (resp. provedená změna zanikne při jejich aktualizaci).

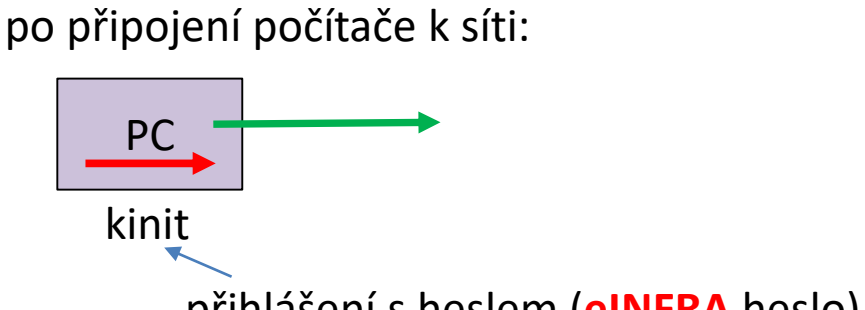
Workflow (pam_krb5)

Počítač je připojen do sítě:



Počítač není připojen do sítě:





Doporučení:

- Vhodné pro notebooky nebo počítače mimo eINFRA**.**
- **Lokální** heslo je nutné **nastavit před** instalací balíčku ncbr-personal-authc-einfra (tj. při instalaci počítače nebo pomocí příkazu passwd).
- Je vhodné mít **stejné lokální a eINFRA** heslo.

Cvičení 4

1. Zprovozněte si podporu pro vytváření kerberovských lístků do realmu META virtuální organizace MetaCentrum ve vaší instalaci Ubuntu server (bod 1 a 2 předchozího návodu).
2. Ověřte, že můžete vytvořit kerberovské lístky příkazem kinit a klist.
3. Upravte si nastavení příkazu ssh pro použití kerberovských lístků (bod 3 předchozího návodu).
4. Ověřte, že se můžete přihlásit na libovolný čelní uzel MetaCentra nebo klastru WOLF bez použití hesla.
5. Ověřte, že se kerberovské lístky přenášejí na čelní uzel.
6. Zprovozněte si vytváření krb5 lístku při prvotním přihlášení (bod 4 předchozího návodu).
7. Ověřte příkazem klist, že máte po přihlášení vytvořené kerberovské lístky.
8. Přihlaste se do virtuálního stroje pomocí ssh z hostitelského stroj. Je vyžadování heslo? Proč nemáte vytvořené krb5 lístky?
9. Stáhněte si balíček ncbr-krb5-einfra a prozkoumejte jeho obsah pomoci programu *mc*.

Instalace Kerbera pro realm META

manuální instalace

Instalace Kerbera (klienti)

Klientskou část Kerbera je možné instalovat na libovolný počítač, který je připojený do internetu. Níže uvedený postup je otestovaný v OS Ubuntu 16.04 LTS.

1) Instalace NTP (Network Time Protocol daemon and utility programs) – je nutné pro správné nastavení času (během konfigurace zvolte výchozí hodnoty)

```
$ sudo apt-get install ntp
```

2) Instalace klientských utilit systému Kerberos (během konfigurace zvolte výchozí hodnoty)

nebo heimdal-clients

```
$ sudo apt-get install krb5-user
```

3) Získání konfiguračního souboru krb5.conf pro MetaCentrum. Soubor si můžete zkopírovat z libovolného čelního uzlu MetaCentra nebo libovolného uzlu klastru WOLF. Jeho umístění je /etc/krb5.conf

4) Soubor zkopírujte (jako super uživatel) do /etc/krb5.conf.META a nastavte mu práva 0666 (pouze pro čtení).

5) Vytvořte symbolický odkaz:

```
$ sudo unlink /etc/krb5.conf
$ sudo ln -s /etc/krb5.conf.META /etc/krb5.conf
```

Integrace Kerbera do ssh

Použití kerberovských lístků pro vzdálené přihlašování na uzly MetaCentra je nutné povolit v konfiguraci příkazu **ssh** (změna platí i pro příkaz **scp**). Změnu je možné udělat pro všechny uživatele změnou souboru **/etc/ssh/ssh_config** nebo změnou/vytvořením souboru **~/.ssh/config** pro konkrétního uživatele.

neměňte výchozí zakomentované (#) hodnoty změny uvádějte nakonec

```
Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
...
    SendEnv LANG LC_*
    HashKnownHosts no
    GSSAPIAuthentication yes
    GSSAPIDelegateCredentials yes
    ForwardX11 yes
```

povolí autentizaci pomocí kerberovského lístku, tuto formu autentizace musí podporovat vzdálený stroj

přenese lístek(y) na vzdálený stroj

umožní použít doplňování názvů strojů u příkazu ssh a scp pomocí TAB

automaticky exportuje X11 display (ekvivalent volby -X)

ssh a kerberos

Pokud máte **v eINFRA jiné přihlašovací jméno** než na výchozím stroji, tak jej musíte explicitně uvést při použití **ssh** příkazu. Druhou možností je změna konfigurace ssh pomocí souboru **~/.ssh/config**, viz man ssh_config, položka **User**. Při použití druhé možnosti je nutné minimálně nastavit **GSSAPIAuthentication** a **GSSAPIDelegateCredentials** (viz výše).

~/.ssh/config

```
Host skirit.ics.muni.cz tarkil.cesnet.cz
    User xstepan3
    SendEnv LANG LC_*
    HashKnownHosts no
    GSSAPIAuthentication yes
    GSSAPIDelegateCredentials yes
    ForwardX11 yes
```

seznam jmen čelních uzlů oddělených mezerou

přihlašovací jméno do MetaCentra

přístupová práva pro soubor **~/.ssh/config**,
pro skupinu a jiné – maximálně jen právo pro čtení