C2110 *UNIX and programming*

Lesson 2 / Module 1

PS / 2020 Distance form of teaching: Rev1

Petr Kulhanek

kulhanek@chemi.muni.cz

National Center for Biomolecular Research, Faculty of Science
Masaryk University, Kamenice 5, CZ-62500 Brno

Kerberos

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

i.e., why doesn‘t it want a password from me?

More detailed information in course C2115.

Kerberos

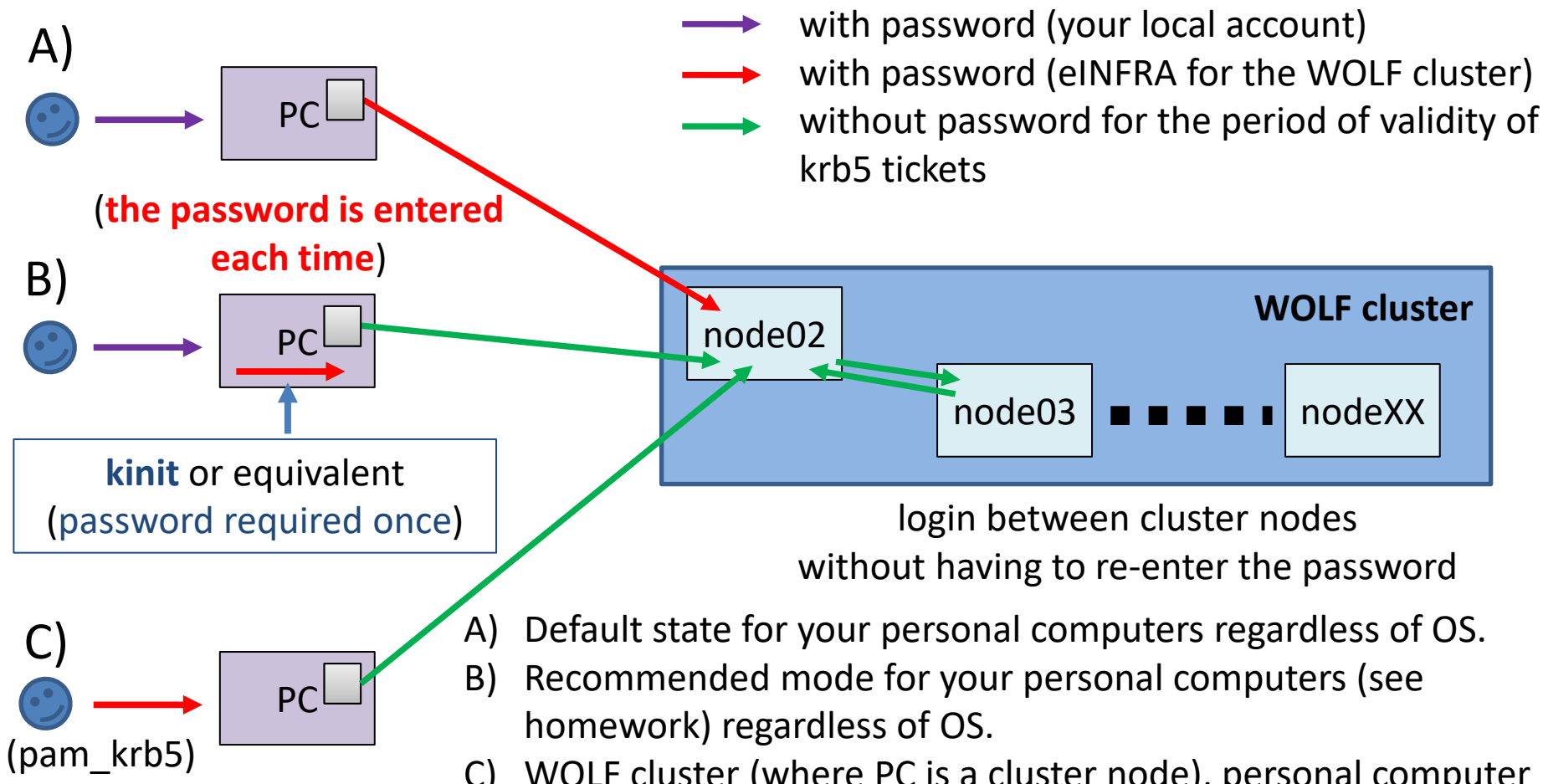
On the WOLF cluster, **Kerberos system** is used to verify the user's identity. After primary authentication (login/password), the user gets a ticket from the realm **META**, which entitles it to use of cluster services or to log in to other clusters using the same authentication realm without re-entering the password (e.g., MetaCentrum) for the entire duration of the ticket.

Kerberos is a network authentication protocol that allows anyone communicating on an insecure network to securely prove their identity to someone else. Kerberos prevents tapping or repetition of such communications and ensures data integrity. It was created primarily for the client-server model and provides mutual authentication - both the client and the server verify the identity of their counterpart. Kerberos is built on symmetric cryptography and therefore needs a trusted third party. Optionally, it can use asymmetric encryption in certain parts of the authentication process.

Kerberos has a **strict time synchronization requirements for clients and servers**. Tickets have a given lifetime, and if the client's time is not synchronized with the server's time, authentication will fail. The default setting by MIT requires these times **not to differ by more than 5 minutes**. In practice, **NTP (Network Time Protocol)** daemons are used to synchronize the clock.

wikipedia.org

Workflow



A) Default state for your personal computers regardless of OS.

B) Recommended mode for your personal computers (see homework) regardless of OS.

C) WOLF cluster (where PC is a cluster node), personal computer with Linux OS (recommended configuration for serious work), details C2115

!!! In an environment that uses krb authentication, ssh keys are NOT RECOMMENDED !!!

Ticket Expiration

If the ticket expires, further access to the services that require it will be denied. This can lead to visible errors with denied access. **However, some errors are not obvious and finding the cause may not be "easy"**. Typically, this situation occurs for sessions that are open longer than is the validity of Kerberos ticket and mainly concerns software activated by the module command, which is physically located on the AFS file system (almost most software in MetaCentrum and on the WOLF cluster).

If something starts to behave strangely (malfunctioning software modules), first check that you have valid Kerberos tickets (klist) and recreate them if necessary (kinit).

Commands

kinit creates a new Kerberos ticket

klist lists existing Kerberos tickets

kdestroy removes existing Kerberos leaves

On the WOLF cluster, Kerberos tickets are created during initial login and are refreshed each time a session is unlocked.


```
[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 ~]$
```

Exercise 1

1. Log in to the workstation wolf03.ncbr.muni.cz (ssh, putty, etc.).
2. Have you received Kerberos tickets? Check their status (**klist**). When will they expire?
3. From machine wolf03, log in to machine wolf06 with the command ssh. Is a password required?
4. Have you received Kerberos tickets? Check their status (**klist**). When will they expire?
5. Log out of the wolf06 machine (exit).
6. Repeat the tasks (points 3, 4, 5), but first remove the tickets on the wolf03 with the command **kdestroy**.
7. Repeat the tasts (points 3, 4, 5), but first restore the tickets on the wolf03 with the command **kinit**.
8. If you have an account in MetaCentrum, log in to skirit.ics.muni.cz from wolf03. Is a password required?

Homework

Homework

1. On your personal computer, setup variant B of the workflow from page 4. You will find the procedure in the accompanying presentation according to the type of OS on your computer.