Kerberos and NFS4 on Linux

isginf Workshop

Welcome

- First workshop we organize!
- Background info and three practical labs
- **Goal is to show you how to get NFS4 with Kerberos working on your Linux systems**

👍 Get coffee and sweets before we start! 👍

Kerberos

Kerberos

- Actually *Kerberos 5* or *V*
- Ticket based authentication system with a central authentication service
    - Often called *Single Sign On* (*SSO*) in business IT language
- The *Key Distribution Center* (*KDC*) as central service
    - Has a database of all user credentials and services

Kerberos Realm

- Each *KDC* has ist own *Realm*
  - **Active Directory** (**A**D) calls this *Domain*
- The ITS **AD** uses the *Realm* or *Domain* is `D.ETHZ.CH`
  - **AD** also uses the short name `D`
- KDC only reachable from ETH networks
  - Use VPN otherwise

Kerberos Principals

- *Principals* are unique names in the *Realm*
- **Active Directory** knows three types of principals:
  - Users (`hmuster`)
  - Computers (`server$`)
  - Services (`service/server`)
- *Service principals* are typically held by computers
  - All princpals of a user have the same keys

Kerberos Tickets

- *Token* for a *principal* with a defined life time and purpose
  - Replace a password when accessing a service
  - Security trade-off
- Two types of tickets
  - *Ticket Granting Tickets* (*TGTs*) held by users to obtain *Service Tickets*
  - *Service Tickets* presented to servers to access a service
- Obtaining a TGT often used for simple authentication

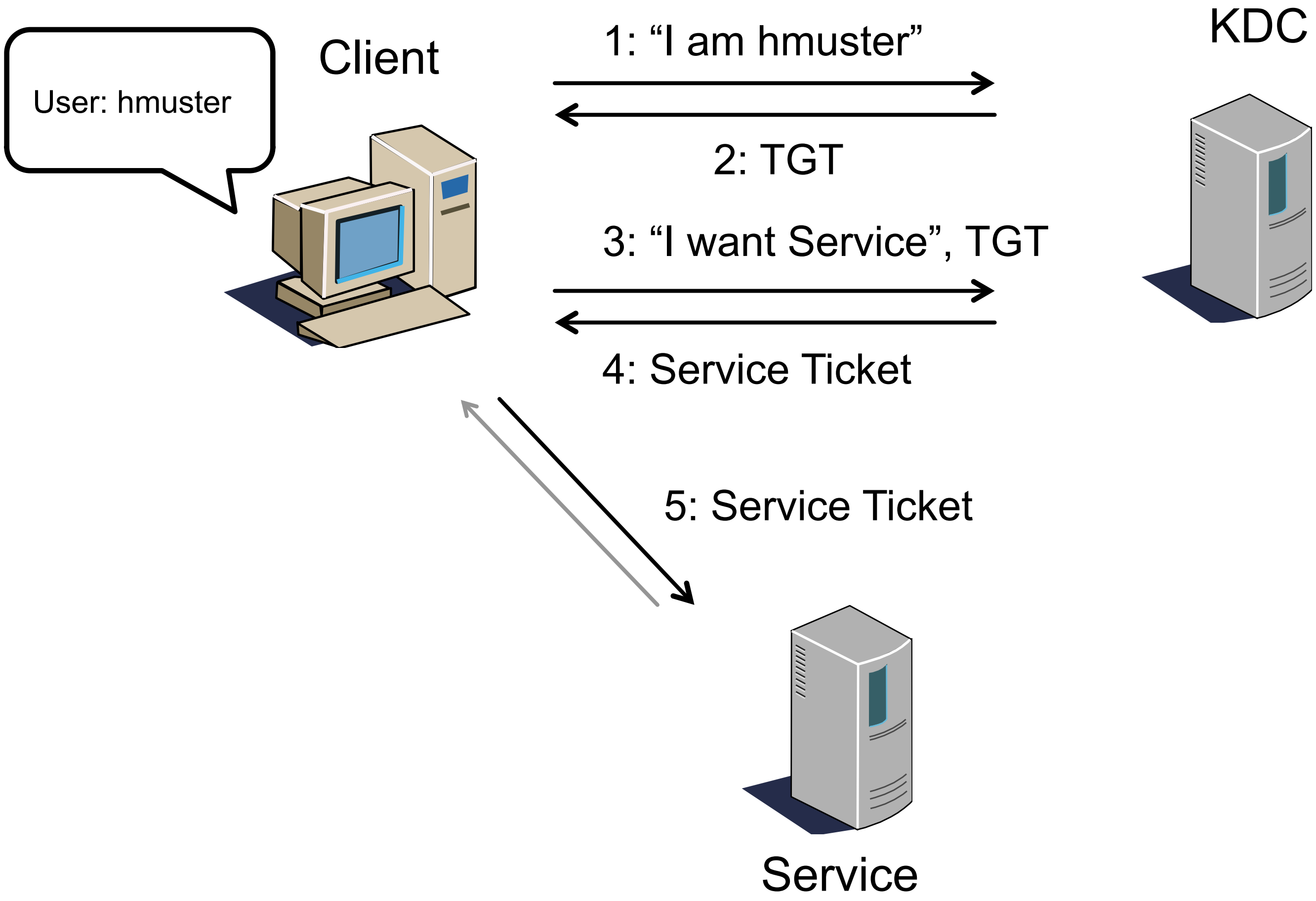
Kerberos Ticket Properties

- *TGTs* have two lifetimes
  - Initial lifetime is 10 hours (at ETH)
  - Can be renewed for 7 days (at ETH) without password if still valid
  - Often done in the background (`krenew`, `sssd`, `Gnome`)
  - Service tickets have a 1 hour lifetime (at ETH)
- *TGTs* can be forwarded (or not)
  - Important for SSH for passwordless login

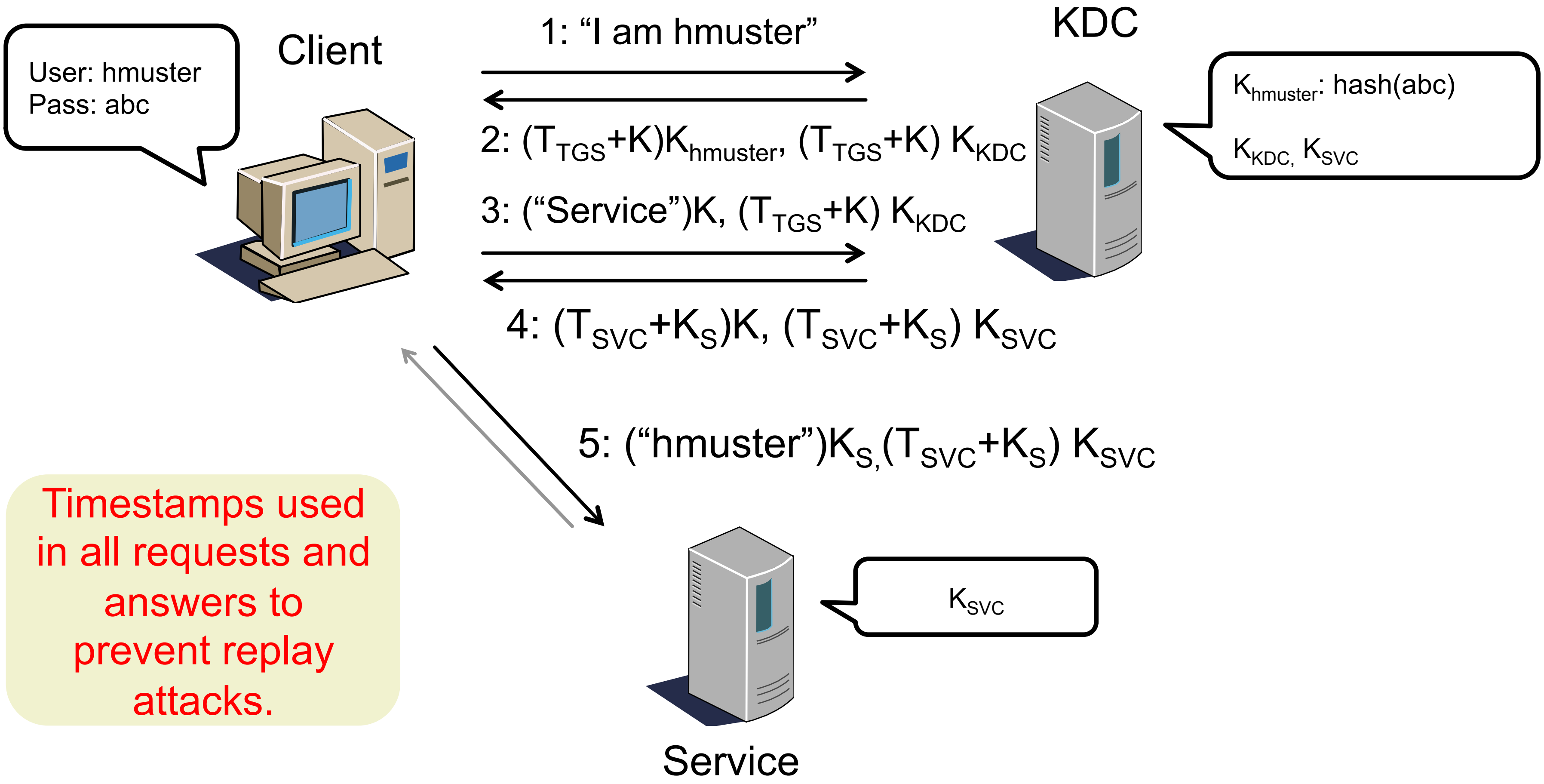
Kerberos Keytab

- A *keytab* contains the *hashed* password of a user principal
  - Actually several hashes, one per encryption type
  - AD knows **five** encryption types, only the two AES variants are secure
- A *keytab* can be used instead of a password
  - `kinit –k –t keytab`
  - Must be kept as secure as the password
  - Keeping a keytab for a user principal only viable on personal systems

Kerberos Protocol Without Crypto



Kerberos Protocol With Basic Crypto


User: hmuster
Pass: abc
Client
1: “I am hmuster”
KDC
$K_{hmuster}$: hash(abc)
K_{KDC}, K_{SVC}
2: $(T_{TGS}+K)K_{hmuster}$, $(T_{TGS}+K)\ K_{KDC}$
3: (“Service”)K, $(T_{TGS}+K)\ K_{KDC}$
4: $(T_{SVC}+K_S)K$, $(T_{SVC}+K_S)\ K_{SVC}$
5: (“hmuster”)$K_{S,}(T_{SVC}+K_S)\ K_{SVC}$
K_{SVC}
Service

Timestamps used in all requests and answers to prevent replay attacks.

Active Directory Implementation

- PAC in TGTs
  - Holds information about the user at the time of authentication
    - Policies, **member groups**, etc.
  - Used by MS systems and the ITS NAS, do not disable
- Joining Computers to the **AD**
  - Typically using an admin account (insecure for network deployment)
  - Secure alternative using web service of *isginf*

Kerberos in Linux

- Basic Kerberos support
  - `kinit`, `klist`, `krenew` and friends
- Services that support authenticating **against** Kerberos
  - SSH, apache, web applications
- Services that support authentication **using tickets**
  - SSH, NFS4, SMB/CIFS

Lab 1

Preparation

- Start here:

  https://www.isg.inf.ethz.ch/Main/AboutUsActivitiesWorkshopsKerberos

  or

  https://www.isg.inf.ethz.ch ➔ **About us ➔ Activities ➔ Workshops ➔ Kerberos and NFS4 on Linux Workshop**

- **First do all the preparation steps before going to Lab 1**

Login and Kerberos

Login In General

- Goal: Any login should create a ticket
  - Needed for home directories using NFS4 with Kerberos
- Need to set up PAM and SSH
- Tickets should also be renewed
  - `sssd` does this automatically, except when using SSH
  - Some desktop extensions also do this

SSH

- OpenSSH `sshd` works with Kerberos
  - Create a ticket after login (with password or forwardable ticket)
  - Login using a ticket
- OpenSSH sshd does not renew tickets
  - Can use `krenew` to do so
- Public key authentication does not work with Kerberos!
  - Ugly workaround with keytab possible

PAM

- PAM must be set up for all logins
  - Graphical login (`gdm`), SSH
  - Ubuntu and Red Hat distros make it pretty easy
- Instructions for *optional* Kerberos authentication available
  - Try to get a ticket for local users
  - Most distros are configured for *mandatory* Kerberos authentication
  - Local user must use NETHZ user names for this to work

Lab 2

NFS4

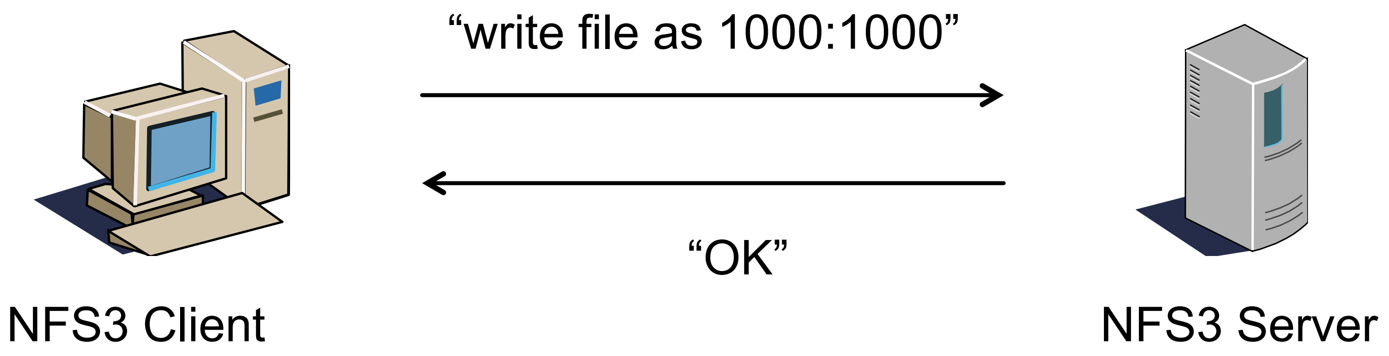
With Kerberos, that is why we are here today

NFS4

- Old protocol from 2000 (NFS3 was from 1995...)
- All traffic over port 2049, client initiated
  - Client does not need special firewall configuration
- Supports ACLs that are somewhat compatible to Windows
- Security part of the Standard
- But: Slower than NFS3, not as wide-spread

NFS3 Insecurity

- I/O commands contain unprotected `uid:gid` for access
  - `root` can become any user...
- NFS3 only allows IP-based security
  - Which does not work with MAC Authentication Bypass (MAB)



“write file as 1000:1000”

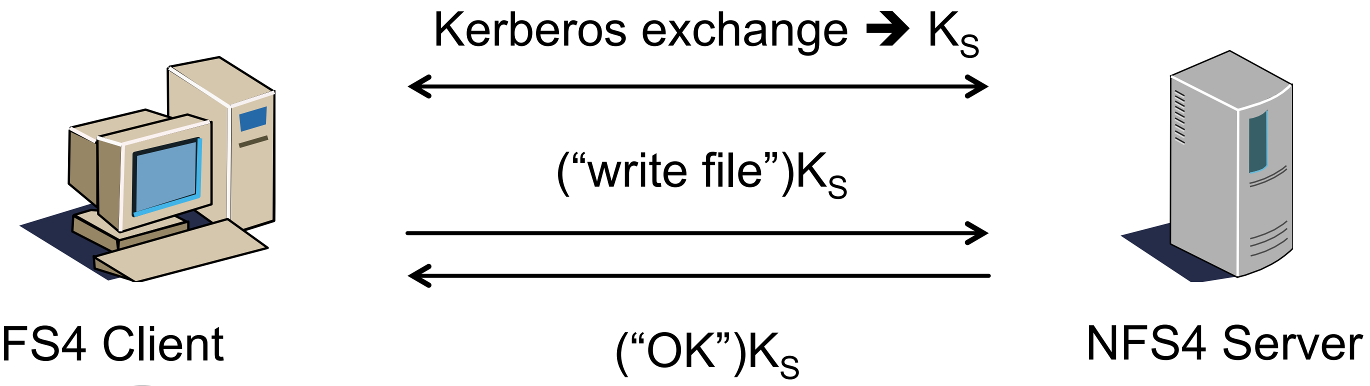
“OK”

NFS3 Client

NFS3 Server

NFS4 With Kerberos

- Session established with Kerberos (session key!)
- All accesses are authenticated (+signed) (+encrypted)
  - `root` can only steal valid tickets on a client



Kerberos exchange ➔ K_S

(“write file”)K_S

(“OK”)K_S

NFS4 Client

NFS4 Server

Mounting NFS4 Shares

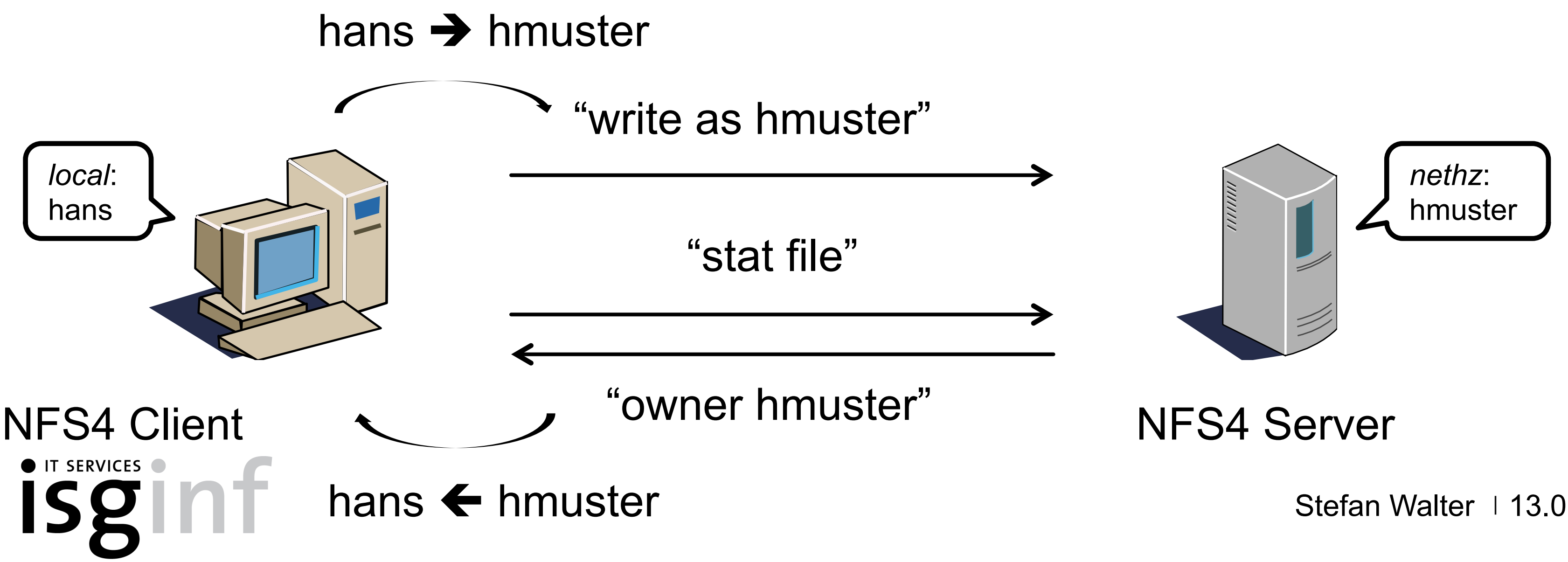
- Mounting a share is simple:

```
mount –o vers=4,sec=krb5p server.ethz.ch:/share /mnt
```

- Three security levels:
  - `krb5`: Just authentication
  - `krbi`: Integrity protection but no enctyption
  - **`krb5p`: Integrity protection and encryption 🡐 RECOMMENDED**
- `krb5i/p` cost ~30-40% load of a CPU core for a 1Gb link

NFS4 Identity Mapping

- NFS4 transfers user/group names not numeric IDs
- ID Mapper used on both sides to translate
  - If names different then rename typically done done by client



hans ➔ hmuster

“write as hmuster”

local:
hans

nethz:
hmuster

“stat file”

“owner hmuster”

NFS4 Client

NFS4 Server

hans ← hmuster

NFS4 Identity Mapping

- Identity mapping requires *NFS4 domain* and *realm*
  - The *NFS4 domain* should be `ethz.ch`.
  - The realm is the AD domain `d.ethz.ch`.
- *Long* names in flight look like this:
  - Users: `hmuster@D.ETHZ.CH@ETHZ.CH`.
  - Groups: `D\hmgroup@ETHZ.CH`.
- But: Plain Linux servers often use short names
  - `hmuster@ETHZ.CH` & `hmgroup@ETHZ.CH`

NFS4 ACLs

- `man nfs4_acl`
- Querying ACLs:
  - `nfs4_getfacl {file}`
- Adding ACLs:
  - `nfs_setfacl –a A::bob@D.ETHZ.CH@ETHZ.CH:R {file}`
- Inheritance:
  - `nfs_setfacl –a A:fd:bob@D.ETHZ.CH@ETHZ.CH:R {dir}`

NFS4 Without Kerberos

- NFS4 also works without Kerberos (`sec=sys`)
  - IP-based security just like NFS3
- Recommended if:
  - Server and client in server rooms
  - Performance is needed
  - Users want to use public key login with SSH

NFS4 Locking

- NFS4 clients must renew locks regularly
- Clients that are away from the network too long lose locks
  - Locks are reclaimed when online again but files may have changed
- Linux has the `nfs.reclaim_lost_locks parameter`
  - If 0 applications get EIO and fail
  - If 1 data corruption may be possible in some cases
- We recommended to set this to 1

Client Requirements

- NFS client utilities with:
  - Correctly configured `rpc.gssd` (does the Kerberos part)
  - Correctly configured ID mapper (plugin required!)
  - NFS4 ACL utilities
- System keytab (or ticket for root) for mounting
- Ticket for each user accessing data on a mounted share
  - Any of the previous methods will do (`kinit`, PAM, ...)

Lab 3

Where To Go From Here

- For personal systems the info on our site should suffice
- If you manage systems for your group, contact us for
  - Configuring `sssd`
  - Joining with real host principal
  - Seting up NSS with LDAP/AD
- Can all be done already now
  - Does not impact current NFS3 client setup

Links

- Kerberos

  https://www.isg.inf.ethz.ch/HelpDesktopsAndLaptopsLinuxKerberos

- NFS4

  https://www.isg.inf.ethz.ch/HelpDesktopsAndLaptopsLinuxNfsV4Server

Questions

and more coffee