



---

Managed by Fermi Research Alliance, LLC for the U.S. Department of Energy Office of Science

---

# Kerberos Infrastructure After Upgrade

Olga Terlyga

Linux at Fermilab

October 29<sup>th</sup>, 2014

# Kerberos Infrastructure After Upgrade

---

On 10/11/2014 we have completed Kerberos Infrastructure Upgrade

- SLF 6.5.
- MIT Kerberos 1.10.3.
- New encryption types added - aes256, aes128, des3.
- No more (obsolete) krb524 service.
- No more CryptoCards

<http://computing.fnal.gov/authentication/kerberos/>

# What broke after upgrade?

---

## pam\_krb5 logins:

- failed while trying to contact krb524 service
- Solution - setting two flags to false in krb5.conf
  - krb4\_convert\_524 = false
  - krb4\_use\_as\_req = false

## Ubuntu kinit md5 error

- Heimdal on Ubuntu is not compatible, install MIT

## AFS aklog:

- /usr/krb5/bin/aklog while trying to contact krb524 service
- /usr/bin/aklog for compound principals due to mapping on AFS servers

<http://computing.fnal.gov/authentication/kerberos/>

# Kerberos Infrastructure After Upgrade

---

Systems administrators:

- Update krb5.conf packages to 5.0a (or later)  
krb5-fermi-config or krb5-fermi-krb5.conf
- If your system is accessed by Mac users directly, re-key host and ftp principals
- If your system has AFS on it, update openafs, all krb5-fermi-\* and kernel; rpms available now.

Users:

- Update krb5.conf
- Mac users need to change their password before upgrading to Yosemite

<http://computing.fnal.gov/authentication/kerberos/>

# Former CryptoCard Users

---

- There is a knowledge base article in Service Now  
“Do I need a CryptoCard replacement?”
- If you DO
  - Request RSA SecurID token through Service Desk.
  - Only **few** hosts that were enabled for CryptoCard login will accept RSA SecurID tokens (FNALU is one)
  - RSA token can only be used to login to the account with the username assigned to the token.
  - RSA token will not issue Kerberos ticket, you will need to run kinit command after logging in.

# Enabling your system to accept RSA SecurID

---

- You will have to download, install and configure PAM module
- Instructions are in Knowledge Base
  - [Making a Linux system accessible without Kerberos \(using RSA SecurID\)](#)
- You will be responsible for updates (download, install)
- We do not have a system in place to notify sysadmins of updates.
- Enabling all systems that were accepting CryptoCards for RSA is not feasible.
- We strongly encourage to configure a “gateway” machine or use fnalu for that purpose.

<http://computing.fnal.gov/authentication/kerberos/>

# Kerberos Infrastructure Upgrade

---

Questions?

# What was tested?

---

**kinit**  
**kdestroy**  
**ssh to old key system**  
**ssh to new key system**  
**ksu**  
**kcroninit**  
**kcon**  
**kcrondestroy**  
**kadmin**  
**kpasswd**  
**k5push**  
**compound principal authentication**  
**compound principal creation**  
**KCA – get certificate**

**NFS – mount share**  
**NFS – write files**  
**Trust access to FNAL from FERMI**  
**Trust access to FERMI from FNAL**  
**Putty**  
**Reflections**  
**NetIDMgr**  
**KCA plugin**  
**CNAS account creation and disable**

# Quick links to configure Kerberos

---

“Strong Authentication at Fermilab” guide in the Knowledge Base

- **Mac OS** - chapter [22](#)
  - download and install /etc/krb5.conf from <http://security.fnal.gov/without-afs-Lion-krb5.conf> or <http://security.fnal.gov/Lion-krb5.conf> (with AFS)
- **Windows** - chapters [19](#), [21](#)
  - download, install MIT Kerberos and putty from <http://computing.fnal.gov/authentication/kfw/>
- **Unix/Linux** - chapters [14](#) , [20](#)
  - download and install krb5.conf from <http://security.fnal.gov/without-afs-krb5.conf> or <http://security.fnal.gov/krb5.conf> (with AFS)

If you need help configuring your Kerberos client,  
open a Service Desk ticket.