Kerberos at Fermilab Upgrade Story

FERMILAB-POSTER-18-104-CD

Fermilab
Authentication Services

Introduction

A Kerberos realm was created at Fermilab in 2000 to allow user authentication without sending clear text passwords over the network. It remains important to have an alternative login method for users that do not have access to a system with Kerberos.

	Systems without Kerberos software	One time password generator
2000s	Internet café, hotel desktop, etc.	CryptoCards
Now	iPad, Android tablet, etc.	? - RSA token

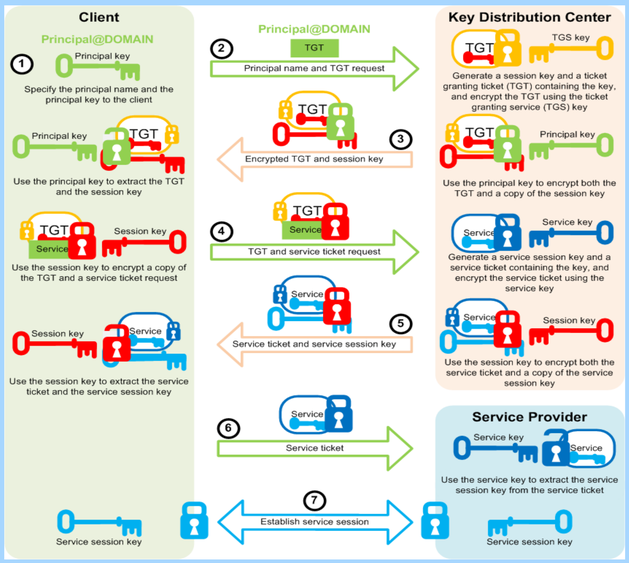
Originally, custom code for CryptoCard support was incorporated into the Kerberos software on the KDCs (Key Distribution Centers). Though this customization was submitted to MIT developers, there was little interest to put it into the official release. Lack of CryptoCard support in new releases was one of the reasons the upgrade was delayed.

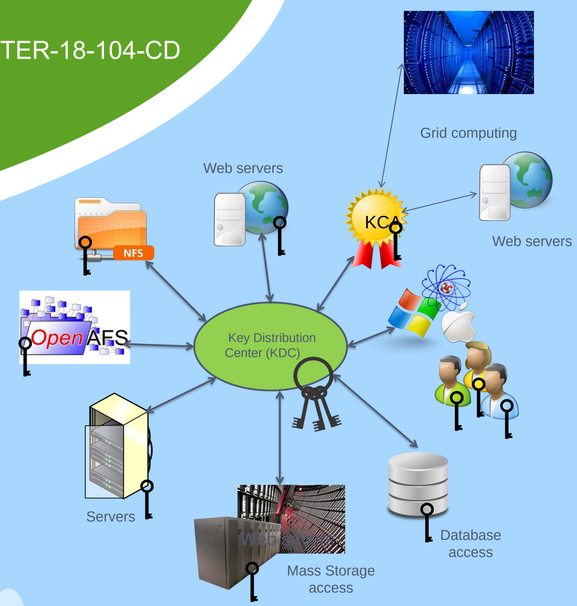
Kerberos Distribution	Advantages	Disadvantages
MIT	Native to Linux	Issues on OSx
Heimdal	Native to OSx interoperates well with MIT	Not native to Linux support effort

The Heimdal distribution seemed like a better fit, so Fermilab was awaiting the 1.6 release. However, at the end of Summer 2014, Apple announced that they eliminated DES encryption support in OSx Yosemite. Therefore Fermilab's Kerberos realm was completely overhauled in a 2-month timeframe with minimal disruption to users. The MIT distribution was used.

Kerberos Protocol

The KDC (Kerberos Distribution Center) verifies authenticity of the user, host or service. Then the KDC issues a session key that encrypts the connection between the user, host or service.

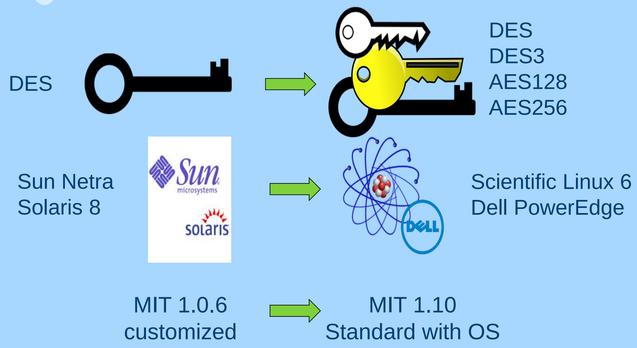




Metrics

- **Master KDC and 14 slaves**
- **94,400** total entries in database
- **15,000** regular users (**6,100** active)
- **28,000** compound principals (automation)
- **45,000** host and ftp principals
- **850** other service principals
- **1-2 millions** requests per day

Upgrade in a Nutshell



What was Tested

We have tested different versions of OSx, Windows and Scientific Linux for users, compound principals, hosts and services with respect to DES and AES keys. All possible combinations cannot be listed here.

Linux Utilities	Windows Utilities	Services	Other
kinit	Putty	ssh (host principal)	AD to Kerberos trust
kpasswd	Reflections	KCA – Kerberos certificate authority	Kerberos to Active Directory trust
ksu	NetId Manager	NFS	Access Control
kcron	KCA plugin	AFS (partial)	Account create/disable (internal tool)
kcroninit			KDC configuration file
kadmin			Client configuration file

Pre-upgrade Challenges

- The master key (stash file) needed to start the KDC service could not be transferred from Solaris to Linux due to the little endian/big endian problem. The workaround involved a combination of Heimdal/MIT kadmin commands on the stash file.
- Direct propagation from the Solaris master to Linux slaves did not work for the same reason. This workaround required a custom script to dump the database and reload it from the file.
- Customizations in the ACL (access control list) file needed to be worked out.
- The krb5.conf file had to be updated on each host well in advance
- We had to re-key every host/service directly interacting with Yosemite users (thousands of machines) - this can be done with one bash command for each host/service
- To preserve trust between the AD (Active Directory) and Kerberos domains we added an additional encryption type to KDC configuration. Adjustments were needed on the AD side as well.

Post-upgrade Issues

- We had issues related to the Kerberos 5 to Kerberos 4 translation service (krb524). Even though this service was not used, it was still running on our KDCs before the upgrade. After the upgrade, it is now unavailable
  - AFS – solution involved switching to standard aklog and adjusting mapping on the AFS side.
  - pam_krb5 – solution involved adding flags to krb5.conf

Summary

Kerberos permeates nearly every aspect of scientific work at Fermilab. Despite the number of systems and environments using our Kerberos for authentication, we were able to perform complete overhaul of Kerberos realm with minimal disruption to users. Unforeseen issues with AFS appeared a day after the upgrade was completed. Our AFS admins worked with our support vendor to quickly resolve the problem. A fully functional test Kerberos realm was undoubtedly the single most important factor in accomplishing this project.

This manuscript has been authored by Fermi Research Alliance, LLC under Contract No. DE-AC02-07CH11359 with the U.S. Department of Energy, Office of Science, Office of High Energy Physics

Presented by:
Olga Terlyga
terlyga@fnal.gov