Multi-Platform User Management and Authentication for Clinical Research

Paul Koppel, David Maffitt, Lawrence Tarbox, Fred Prior
Dept. of Radiology Washington University in St. Louis, MO, USA

ABSTRACT
The IT infrastructure at Washington University's Center for Clinical Imaging Research (CCIR) includes a varied assortment of operating systems (Windows, Solaris, and Linux in various flavors) and application platforms (Apache, Tomcat, PostgreSQL, Oracle, Visual Basic, Java, etc.), with both in-house developed software and commercial systems (scanners, PACS, RIS, etc.). Ideally users would prefer to use the same username/password with all the operating systems and software packages. IT administrators would prefer that a single entity manage users and their access privileges, such that any changes (e.g. to password or privileges) propagate automatically to all systems. The diverse mix of operating systems, platforms, and software packages in CCIR presents an interesting challenge to achieving these goals.

Further complicating the picture is the fact that a given user may have different roles within different projects and trials, with different associated access rights. Most user management subsystems readily handle global roles, but do not easily accommodate project-specific roles. This poster illustrates how we have resolved these issues by deploying a system based on a combination of Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and Kerberos, coupled with extensions to manage project-specific user roles and access privileges.

Kerberos Service

- Provides secure transactions over networks using client-server architecture
- Offers strong user authentication, integrity and privacy
- Can log in to other machines (ssh) or services (apache, tomcat, postgreSQL)
- Authenticate to the service once per session, and subsequent transactions during the session are automatically secured
- Kerberos 5 is the default authentication method in Windows 2003 Active Directory

Initial Authentication and Ticket Granting Ticket

- Client requests a ticket-granting ticket (TGT) from a key distribution center (KDC) that allows it to obtain tickets for services – this can happen at login or using kinit
- KDC checks database and sends a TGT back to the client in encrypted form
- Client uses password to decrypt the TGT and uses it to obtain other tickets for other network services

Service Tickets

- Client requests a service ticket (for example postgreSQL) by sending the TGT to KDC
- KDC sends back to client a service ticket
- Client sends service ticket to server
- Server allows access for client

Kerberos Terminology – Principals

A client in the Kerberos service is called a principal
The KDC assigns tickets to principals
A principal can be a user or a service or a host. For user principals, instance is optional. For service principals, instance is required.

Examples of Principals
pkoppe01@PRIVATE.LAN
POSTGRES/ipswich.private.lan@PRIVATE.LAN
HTTP/ipswich.private.lan@PRIVATE.LAN
host/ipswich.private.lan@PRIVATE.LAN

Realm
A realm is a logical network, similar to a domain, that defines a group of systems under the same KDC. The realm name is the domain name all capitalized. For DNS domain name private.lan, the realm name is PRIVATE.LAN.

Global Roles

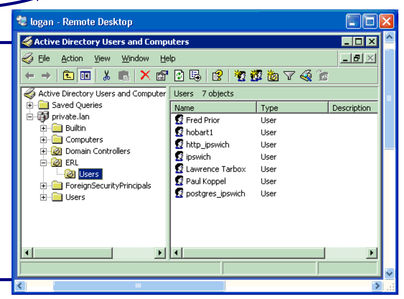
Use AD to authenticate ssh, sftp, su, console login to Red Hat Linux (AS4)

Basic Procedure
- Create /etc/krb5.conf
- Transfer host keytab – use *ktutil* to create */etc/krb5.keytab*
- */usr/bin/system-config-authentication* – select Kerberos
- Create locally locked UNIX user account using *useradd*
- Test by *ssh user@host*

Use AD to authenticate apache web login to Red Hat Linux (AS4)

Basic Procedure
- Transfer http keytab
- make and make install apache2 with
  ./configure --prefix=/usr/local/apache2
- make and make install mod_auth_kerb with ./configure --with-krb4=no --with-krb5=/usr/kerberos --with-apache=/usr/local/apache2
- Modify httpd.conf to use Kerberos

Use AD on Windows Server 2003 SP1 as Kerberos Key Distribution Center (KDC)



Basic Procedure
- Install DNS and Active Directory (AD)
- Create organizational unit (OU)
- Create normal user accounts for Linux hosts, services, and users
- Use ktpass to generate keytab files. Kerberos usernames are multipart. AD usernames are not.
- Create groups to define global roles (e.g. User, Admin, Executive) and group policy.

Use AD to authenticate Windows Client login

Basic Procedure
- Join Windows Domain

Use AD to authenticate tomcat web login to Red Hat Enterprise Linux (AS4)

Basic Procedure
- Transfer tomcat keytab
- Configure tomcat startup script to use Kerberos
- Create jaas.conf, modify server.xml, web.xml

Use AD to authenticate pgSQL login to Red Hat Linux (AS4) PostgreSQL Server

Basic Procedure:
- Transfer postgreSQL keytab
- make and make install postgreSQL with
  ./configure --with-krb5 --with-krb-srvnam=POSTGRES
- *pgsql/bin/createuser user*
- Use "krb5" for database authentication in pg_hba.conf
- Test by *kinit; psql -d db -h host -U user*

Kerberos Tickets after *kinit* and *psql* login

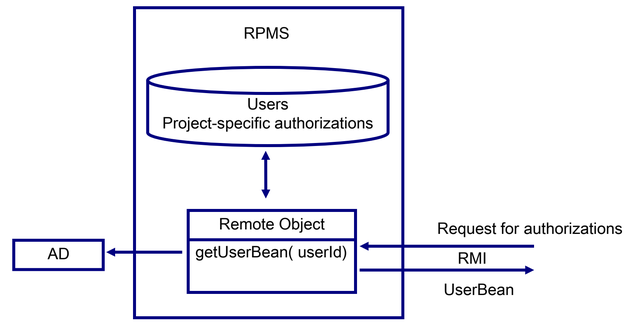
```
[pkoppe01@ipswich ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_501_Unl0dG
Default principal: pkoppe01@PRIVATE.LAN

Valid starting       Expires              Service principal
11/28/06 18:23:15  11/29/06 04:23:19  krbtgt/PRIVATE.LAN@PRIVATE.LAN
        renew until 11/29/06 18:23:15
11/28/06 18:25:08  11/29/06 04:23:19
POSTGRES/ipswich.private.lan@PRIVATE.LAN
        renew until 11/29/06 18:23:15
```

Project-Specific Roles

The Research Project Management System (RPMS) is a custom application that captures complete and detailed information about CCIR projects including scientific goals, scan protocols and custom data entry requirements.

The RPMS is used to record who the project members are and their role on the project (e.g. Principal Investigator, Study Coordinator, and Investigator).

Systems needing to grant project-specific authorizations (e.g. Registration, Scheduling, Data-access Portal) call a remote object on the RPMS. The remote object checks with the Active Directory that the user is a known CCIR member and returns a bean specifying the user's role in a project.



CONCLUSIONS

- Kerberos is a secure method for authenticating users logging into the Linux operating system using ssh, sftp, and console login; and accessing postgreSQL, apache, and tomcat network servers.
- A Windows 2003 server can be used as a KDC and is a convenient system to manage users, their passwords and their global roles.
- Project members and their project-specific roles are recorded in a custom application at the time the project is defined in the CCIR.
- Other systems get user authorization information via remote method invocation on this application.