PAM/LDAP

Wayne Schroeder
Data Intensive Cyber Environments
DICE-UCSD

http://irods.org


THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL


renci

PAM/LDAP

Pluggable Authentication Modules (PAM)
Lightweight Directory Access Protocol (LDAP)

Authenticate Users

Sites can plugin various Authentication Modules into various system services, now IRODS too.

Part of 3.2, extended for 3.3

Typically, users' system passwords.

Security

PAM requires user name and password
  Transferred to iRODS server (agent).
  Get OK/Not-OK returned from PAM.

So iRODS must encrypt this exchange with the iRODS Agent.

We use iRODS password that is created and returned to client.
    A PAM-derived password.

Security continued:

'iinit' needs SSL encrypted session

After 'iinit', other i-commands use regular iRODS-auth iRODS password obfuscation (.irodA file) not system password

Only 'iinit' needs SSL encryption session

The life-time of PAM-derived passwords is set by the admin.

User View

- PAM authentication choice (instead of password, GSI, Kerberos, or OS_Auth)
- 'iinit' and enter their system password
- i-commands use the .irodsA obfuscated password
- In 3.2: generated iRODS passwords valid for 2 weeks (or other defined period)

OS AUTH

- Configured on client hosts
- Users do not enter password
- Verifies that user is logged in
- Uses a SetUID program
- Secure exchange:

  shared secret

  challenge/response
- Part of 3.0
- See 'OS authentication' on irods.org
- Thanks to Chris Smith of Distributed Bio

Password Management

'iinit' if a PAM-iRODS password exists for this user:

- new one not generated
- lifetime of the existing one extended
- and its value returned to 'iinit'
- Useful for multiple clients/hosts

iadmin command to remove pam-derived

iadmin h rpp

Remove irods short-term (ususally 2 weeks) passwords that are created when users authenticate via the iRODS PAM authentication method. For additional security, when using PAM (system passwords), 'iinit' will create a separate iRODS password that is then used (a subsequent 'iinit' extend its 'life'). If the user's system password is changed, you may want to use this rpp command to require the user to re-authenticate.

Next Release PAM/LDAP Authentication Extensions

iinit --ttl time-to-live for PAM-derived passwords

within limits set by admin

Config options to disallow time extensions

each iinit (client host) will get new one

previously, they were not usable but could be extended

Pam-derived passwords are removed when expired

With/for Swedish National Supercomputer Centre

PAM Setup

See 'PAM Authentication' on irods.org

config/config.mk:

PAM_AUTH=1

USE_SSL=1

sudo apt-get install libpam0g-dev

Builds: server/auth/src/PamAuthCheck.c

- Sample/example PAM
- Setuid
- Run by iRODS Agent(server) for Auth
- Is a PAM client

PamAuthCheck.c

Comments describing use
Based on examples
Reads password from STDIN (more secure)
User name on command line
Call PAM client library functions:
  pam_start, pam_authenticate, pam_end
Exits with 0/1
PAM system pauses for invalid password

PAM SSL

PAM SSL Setup page on irods.org

openssl commands to:

- Make RSA key
- Make certificate (or get one from Trusted CA)
- Create the certificate chain
- Generate Diffie-Hellman parameters

Make these accessible to iRODS server

Set environment variables

Possible Client SSL Setup

Wayne Schroeder
DICE-UCSD
schroeder@diceresearch.org
http://irods.org