

Kerberos and PAM

Russ Allbery

May 1, 2007

Contents

- What is PAM?
- The PAM Groups
- PAM for Login
- PAM for Screen Savers
- Kerberos PAM Modules
- Linux PAM Examples
- Solaris PAM Example
- Special Configurations

What is PAM?

- Pluggable Authentication Modules
- Abstracts the user authentication and session setup process
- Only does authentication and simple authorization
- Developed originally on Solaris
- Enhanced but mostly compatible version on Linux
- Now used by many UNIXes, but implementation varies

The PAM Groups

- PAM divides the login process into groups
 - auth: Prompts for and verifies password
 - account: Simple authorization decisions (only for login)
 - session: Prepares for an interactive session
 - password: Handles authentication token changes
- setcred, the odd step-child
- setcred vs. open_session: who knows? who cares?

PAM for Login

- auth group prompts for password, does basic authentication
 - Store the credentials in a separate temporary cache
 - Don't chown credential cache until setcred
- account group does basic authorization
- setcred stores credentials and adds supplemental groups
- session group creates a login session
- When the user logs out, session group closes the login session

PAM for Screen Savers

- auth group prompts for password, does basic authentication
- account group could do authorization, but frequently ignored
- setcred to refresh credentials (REINITIALIZE/REFRESH)
- session group not called
- Bad screen savers don't call setcred and thereby lose

Kerberos PAM Modules

- Sourceforge pam_krb5
- Red Hat pam_krb5
- My pam-krb5, based on Frank Cusack's module
- Solaris native pam_krb5

PAM Configuration

- Debian: `/etc/pam.d/common-*`
- Red Hat: `/etc/pam.d/system-auth`
- Solaris: `/etc/pam.conf`
- Whether to use a Kerberos PAM module for password changes

Linux PAM Example

```
auth      sufficient  pam_krb5.so
auth      required    pam_unix.so  try_first_pass
account   required    pam_krb5.so
account   required    pam_unix.so
session   optional    pam_krb5.so
session   required    pam_unix.so
password  sufficient  pam_krb5.so  minimum_uid=1000
password  required    pam_unix.so  obscure min=6 md5
```

Solaris PAM Example

```
login auth sufficient /usr/local/lib/security/pam_krb5.so
    minimum_uid=100
login auth required /usr/lib/security/pam_unix_auth.so.1
    use_first_pass
login account required /usr/local/lib/security/pam_krb5.so
    minimum_uid=100
login account required /usr/lib/security/pam_unix_account.so.1
login session required /usr/local/lib/security/pam_krb5.so
    retain_after_close minimum_uid=100
login session required /usr/lib/security/pam_unix_session.so.1
```

(no wrapping)

Special Configuration

- `minimum_uid` or `ignore_root`
- MIT Kerberos needs `master_kdc` setting for password expiry
- SSH and ticket cache initialization
- SSH and `ChallengeResponseAuthentication`
- `search_k5login` and shared role accounts
- PKINIT
- AFS — see talk on Friday