University of Michigan Site Report

Thomas L. Kula

Information Technology Central Services

University of Michigan

2009 AFS and Kerberos Best Practices Workshop

Kerberos

Kerberos

- On 28 February 2009 at 39 minutes and 22 seconds past midnight EST UMICH.EDU became entirely Kerberos 4 free

Kerberos

- Update to MIT Kerberos 1.6.3
- Down to 14 local patches
- Large patches are: umich style replication, the weird way we do referrals, password quality plugin

Kerberos

- Deploy password quality plugin framework based on what Stanford used with 1.4 series MIT kerberos

Kerberos

- 2007: about 330K principals
- 2009: just over 400K principals

Kerberos

- Five KDCS

- – three in one machine room (hey, they're in separate rows now!)
  – one on the other side of campus
  – one on the Dearborn campus
  – * which works just fine
    * and got us a thanks when our inter-campus link went down

Kerberos

- Fortunate in that kerberos is pretty entrenched in people's minds here
- Helped in no small part by Cosign
- It's how I get in to report my hours in the Peoplesoft web interface....

Kerberos Security Audits

- Work with ITSS (IT Security Services, a separate (for now) office)
- Twice-yearly audits
- John the Ripper
- Really need to figure out how to get JtR to work with non-AFS keys....

Kerberos Security Audits

- We identify weak passwords
- ITSS asks departments to opt-in, provides departments with lists of users with weak passwords
- Departments contact user
- ITSS tells us who to set bits on

Kerberos Security Audit

- This last run we got two of the larger units on campus to opt-in

- College of Engineering and MCIT

Kerberos Security Audit

- 2007: about 330K principals, 6.25% identified as weak
- 2009: about 400K principals, 2.67% identified as weak

Kerberos: problems of scale

- With 400K principals, 1% is 4000
- We often run into issues where we're down to the last few percent of principals, and only 1 or 2 % is 4 - 8000 principals, too many to deal with manually

AFS

AFS

- "I'm not dead yet!"
- Despite standard "just replace it with X", still going strong

AFS Growth

- In the last 12 months:
- Started with 41TB capacity, 22TB used
- Ended with 77TB capacity, 40TB used
- 225K increased to 243K volumes

AFS Growth

- In the last 12 months:

- default and move everyone to 10GB home volumes

AFS Growth

- Some production volumes over 100GB in size
- Still don't want to go too large
- "No blink limit" is 50GB
- May make that larger when have better operational experience with new fileserver hardware

AFS Deployment

- 1.4.8 with patches (mostly shadow stuff)
- 3 db servers (hey, at least they are in different rows now!)

AFS Deployment

- 3 letter volumeifrastructure volumes servers
- 8 small fileservers (experemental, becoming dedicated group volumes)
- 18 large fileservers, 3 1.5TB partitions
- spread between two sites on either side of campus

AFS Shadows

- Shadowing about 15% of our volumes
- Shadow nightly
- Have yet to do a live instance test of it, but plan on doing this year
- Intend on replacing our disaster recovery system with shadows, eventually

AFS

- We got tired of making test cells by hand
- Finally sat down, used radmind to make it fairly easy for us to bring up a test cell
- The hardest part is finding hardware, and a place to put it
- Hope virtualization stuff will make that easier in the future

AFS Major Headaches in the last year

- ext3 corruption makes us sad
- RT124097, issue with the `hostList` (it seems) caused us a headache earlier in the year, still working on that

Working with the AFS Community

- We've contributed some patches and bug reports
- Worked with OpenAFS folks as well as folks at other sites
- Had a generally good experience with that
- Wish we had resources to dedicate to more testing, especially of features we really want.

Random Stuff

Database Backups

- Getting ready to deploy setup to do consistent database backups
- Kerberos: non-advertised slave kdc
- AFS: clone db server

Remctl

- We're basing more of our infrastructure on remctl
- Managed to get someone from another part of campus excited
  - "You mean I could run this as well?"

Remctl

- Using to delegate and automate things that would have had to been done manually in the past
- Group Home Directory creation, Accounts Office/ITSS principal disable tool
- Ideal for fine-grained sane privilege escalation