How We Deleted Two-Thirds of Our User IDs and Lived to Talk About It!

David Buehl
Fred Lates
Phil Peters

z/OS Platform Evaluation Test / Integration Test

Agenda

- Who are we?
- Our environment
- Why this was done
- Initial pass at identifying owners of active user IDs
- Automated reports
- Active user IDs that appear to be inactive
- Safeguards
- Non-RACF components
- Results

Who are we?

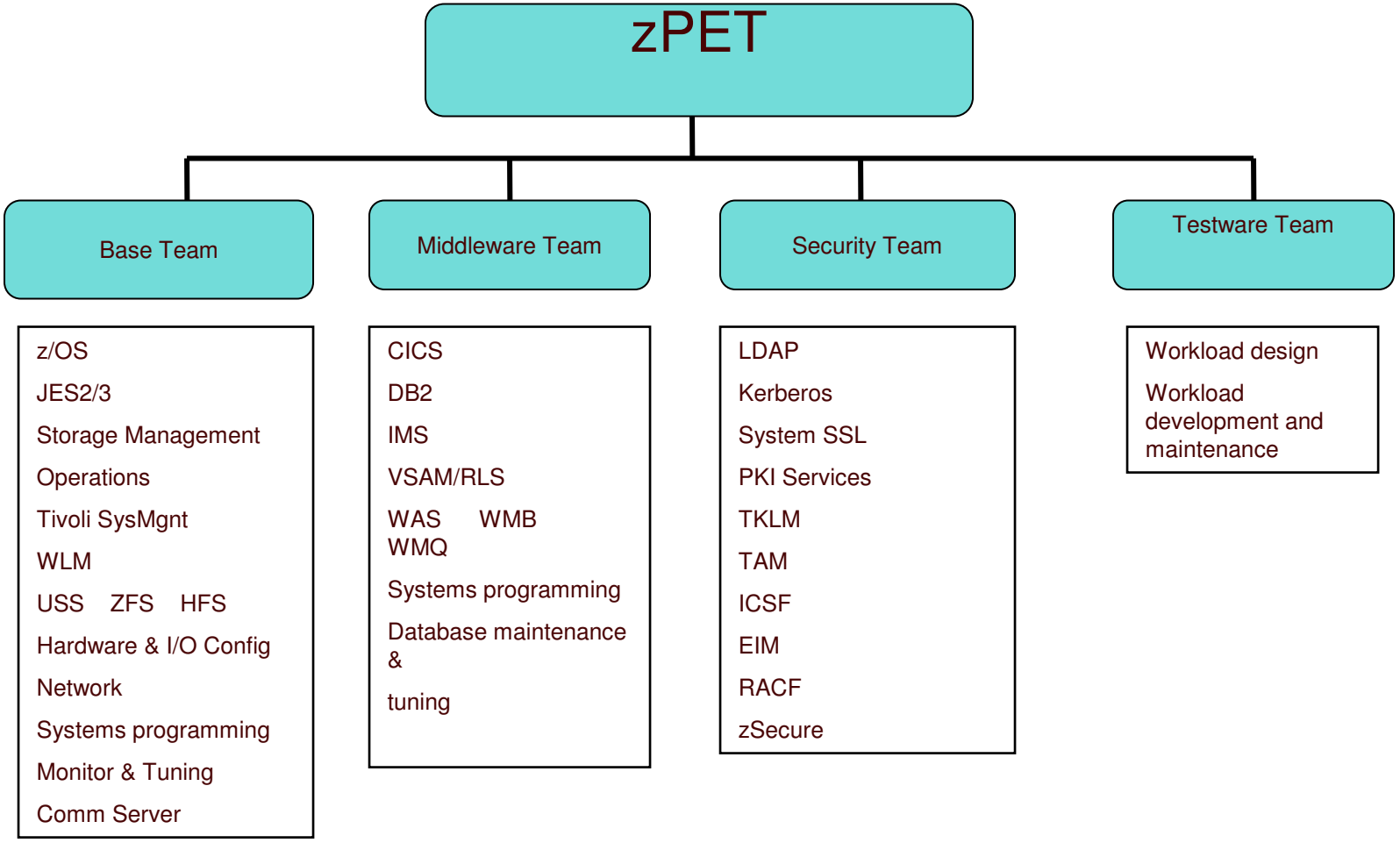
zPET is …….

- zPET = zSeries Platform Evaluation Test
- the first “true” z/OS client
- the proving ground for most of IBM’s zSeries products – it is our responsibility to ensure its quality, functionality, usability and serviceability

zPET will continue to …..

- evolve based on product directions and client needs
- share its experiences (painful or otherwise) with its clients
- collaborate with the development teams and provide them with a client’s perspective

Who are we? – Our Organization Structure



Who are we? – Our Mission Statement

- Install, deploy and manage solutions (Integration Test) in a z/OS Parallel Sysplex environment to ensure that quality, functionality, usability and serviceability characteristics meet client requirements
- Understand and advocate the clients' viewpoint
- Share with others the system perspective, insights and knowledge uniquely gained by working in complex operating system environments.
- Provide feedback to the development labs to ensure a high quality product
- Identify and assist in the removal of defects

Who are we? – Methodology

- Focus on cross-product interaction and dependencies
- Run a pseudo-production shop (dedicated H/W resources) using IBM products and running real client applications
- Run high-volume, high-stress environment
- Provide 24x7 availability to simulated end users
- Use product documentation in performing migration and exploitation of new functions
- Use IBM recommended best practices for service and product migrations.

Who are we? – Deliverables

- Validate z/OS based solutions through integration test
- Influence Brand & Development on new line items and product directions bringing to the table the clients' viewpoint
- Document our test experiences in the zSeries Platform Test Report for z/OS and Linux Virtual Servers to share them with clients
  http://www.ibm.com/systems/services/platformtest/servers/systemz.html
- Assist clients by using team members' expertise e.g. customer engagement, advocacy, etc…
- Present in technical conferences i.e. Share…
- Produce White Papers.
- Identify HW & SW defects, provide data to L2/Dev and test fixes

Our Environment

- 2 Parallel Sysplexes each with their own RACF database
- RACF Databases 20 years old
- No "customers" on system -- just Support/Test team
- No formal ownership of user IDs
- Over 22,000 user IDs in one RACF environment
- Over 26,000 user IDs in other RACF environment
- No previous cleanup activities

Why This Was Done

- Attending RUG meetings
- Role Based Security (ITIM)
- Identify ID owners
- Good practice
- Publish experiences

Initial Pass at Identifying Owners of Active User IDs

- Made educated guess at ownership of <100 TSO user IDs
- Based on user ID, name or owner fields or group connections
- Sent email to team asking for confirmation
- If response indicated ID not needed, updated DATA field with "Marked for deletion"
- If response indicated ID was needed, updated DATA field with "2009 -- owner's name -- purpose"

Automated Reports

- Ran two daily jobs to list user IDs that did **not** have "2009" in DATA field and had either:
  1) a recent last access or last connect date
  2) an SMF occurrence from previous day
- Tracked down owners for any IDs in reports and updated DATA field with owner info
- Need to check for both cases since some applications might not cut SMF records and some might not update statistics
- Need to also consider case where application doesn't do either

Active User IDs that Appear to be Inactive

Caused by applications that do not cut SMF or update last access

eg. RACROUTE REQUEST=VERIFY, STAT=NO,LOG=NONE

Some possible ways of handling:

- If applications that do this are known, ask app owner what IDs use them
- Turn on UAUDIT for IDs that are to be deleted
- Use a tool such as zSecure Access Monitor that shows all accesses
- Publish list of user IDs to be deleted before actual delete

Safeguards

- Ran reports for almost a year before deleting IDs
- Revoked the IDs and removed all privs and accesses before deleting
- Split overall list of IDs to delete into smaller lists
- Nightly copies of RACF databases taken

Non-RACF Components

- Datasets:

  -Deleted basic datasets such as ISPF.PROFILE

  -Renamed others under OLDHLQ hlq and migrated to tape

  -If dataset actively being used but ID not needed, created a group for the hlq
- Aliases were deleted
- USS:

  -Deleted filesystems

  -Removed directories where the filesystems were mounted

Results

- Deleted 33,000 user IDs across the 2 sysplexes
- Identified owners for remaining 15,000 user IDs
- Two occurrences of an ID being needed after it was revoked
- No datasets had to be recovered
- Continue to run daily reporting jobs
- Closer control of ID administration now
- Plan to run IRRUT400 to reblock database