Open VMS Environments

Robert Gezelter, CDP CSA, CSE

Principal

Robert Gezelter Software Consultant http://www.rlgsc.com

The rules

- Often, the best way to learn is by doing
- This “Hands-on” will be in the form of a “game”
- In this game, each attendee plays the role of a departmental administrator on a shared, multi-architecture OpenVMScluster.
- There will be one overall system manager (either an attendee or one of the instructors)
- There will be a CIO, likely your lead instructor, who will make high level choices.

The scenario

- Business Organization with tens of departments
- Small (1-3) system management team.
- Imperative to reduce number of persons holding privileges from:
  - Corporate management
  - CIO (decentralization of responsibilities to the extent possible)
  - **Auditors (both company-hired and regulatory)**

The system

- Mixed Architecture OpenVMS Cluster
  - **ALFA** Alphaserver (courtesy of HP)
  - **VICTOR** VAXserver (courtesy of Nemonix)
  - **INDIA** Itanium (we couldn't arrange for one for this class, but the principles are the same --- OpenVMS is OpenVMS!)
- 100 Mbps IEEE 802.3 Network
- For convenience, the "user" disks reside on the Alphaserver (in a production environment, they would be on external storage controller, likely connected using FibreChannel).

The goal

- System management without privileges
  - Admittedly, some tasks require privileges
  - But such tasks are not the majority of system management
- Fine control of access to programs and data
- Division of responsibility

The tasks

- Customize user environment by department and/or applications
- Control user access to different nodes in the cluster
- Control access to files on an individual user basis
- Manage batch queues
- Manage print queues

Your accounts

- You will draw two index cards associated with your role:
  - The larger card is a “sign”, identifying your role in the game to your colleagues
  - The smaller card has the account information associated with that role.
  - The smaller card will have three additional accounts for each and every student:
    - A normal user account in your department
    - An account in a generic group other than your primary identity
    - An account in the IT group with rights needed to be an alternate departmental administrator

Your accounts

- Each account has three privileges:
  - **`TMPMBX`** – Temporary Mailbox
  - **`NETMBX`** – Network Mailbox
  - **`OPER`** – Operator functions
- None of the problems will require more than the above

A small scheduling note

- There are more problems in this collection than can be done in the 4 hours (with breaks)
- We are not going to rush. The rate at which we can do problems depends upon many elements, including class size
- We expect to finish approximately six problem sets

The problems

- Controlling logons – Group Logon Scripts
- Controlling access:
  - Data files
  - Applications
  - Queues

The mechanism

- Most system managers are fairly familiar with OpenVMS – classic security:
  - System (groups <= **MAXSYSGROUP**, or **SYSPRV**)
  - Owner (the UIC of the object's creator)
  - Group (users whose group is the same as the creator)
  - World (users who are not members of the categories above)
- Fewer are familiar with Identifier-based security
- **Identifier-based security** will be used as our basis for implementing **authorized capabilities**. DCL and ACLs will be our tools for accessing and manipulating Identifiers.

The tools

- **`F$GETJPI("", "RIGHTLIST")`**
- **`SET ACL …`**
- Rooted, concealed logical names
- Hierarchical directories

Questions?

Robert Gezelter, CDP CSA, CSE

Principal

Robert Gezelter Software Consultant http://www.rlgsc.com

HP WORLD 2004

Solutions and Technology Conference & Expo

Co-produced by:

interex

shared knowledge • shared power

encompass

AN HP USER GROUP