#SHAREorg

SHARE
Technology · Connections · Results

New: sudo for z/OS

Richard Theis (rtheis@us.ibm.com)
IBM Rochester, MN

March 13, 2012
Session 10637

Trademarks and Disclaimers

- **See http://www.ibm.com/legal/copytrade.shtml for a list of IBM trademarks.**
- **The following are trademarks or registered trademarks of other companies**
  - UNIX is a registered trademark of The Open Group in the United States and other countries
  - CERT® is a registered trademark and service mark of Carnegie Mellon University.
  - ssh® is a registered trademark of SSH Communications Security Corp
  - X Window System is a trademark of X Consortium, Inc
- **All other products may be trademarks or registered trademarks of their respective companies**

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Agenda

>> Overview <<

Packaging and installation

Usage

Examples

Appendix

Overview

- **What is sudo?**

  sudo (su “do”) is an open source tool that allows a system administrator to delegate authority in order to give certain users (or groups of users) the ability to run some (or all) commands as a superuser or another user, while providing an audit trail of the commands and their arguments. It is a command-line UNIX application.

Overview

- **Problem Statement**
  - z/OS system administrators need a more granular and flexible method to minimize user privileges while still allowing users to get their work done.
- **Solution**
  - IBM ported the sudo open source tool to z/OS. sudo is commonly available on other UNIX/Linux platforms.
- **Benefits**
  - sudo for z/OS is designed to allow a z/OS system administrator to minimize user privileges while still allowing users to get their work done. **sudo for z/OS** is preferred over **su** since it doesn't require giving the invoking user "open" access to run as the target user.

Overview

- **Benefits (Continued)**
  - Today without sudo for z/OS, a z/OS system administrator could…
    (1) Allow users to share UID(0)
    (2) Allow users to be surrogates of a UID(0) user
    (i.e. **su –s <user>)**
    (3) Provide users with a UID(0) user's password (i.e. **su <user>**)
    (4) Give users BPX.SUPERUSER authority
    (i.e. **su** superuser mode)
    (5) Give users select UNIXPRIV authorities

    However, all of these options have inherent risks associated with them. They may provide a user with more privilege than the system administrator wants to provide. These risks result in the need for sudo for z/OS.

Overview

- **Benefits (Continued)**
  - sudo for z/OS doesn't require sharing UIDs or passwords, creating surrogates or granting excessive authority in order to allow users to get their work done. Additional customizations are possible, including the ability to have users run as non-UID(0) users.
  - sudo for z/OS has built-in logging of commands that are being run under the sudo authority.

Overview

- **Who maintains sudo and where can I find more information?**
  - IBM ported open source sudo version 1.7.2p2 to z/OS and modified the port for better z/OS integration.
  - Refer to http://www.ibm.com/systems/z/os/zos/features/unix/ported/suptlk/ for sudo for z/OS.
  - Refer to http://www.sudo.ws/ for open source sudo.

Agenda

Overview

>> Packaging and installation <<

Usage

Examples

Appendix

Packaging and installation

- **sudo for z/OS has been provided via APAR OA34949 (PTF UA59179) to IBM Ported Tools for z/OS: Supplementary Toolkit for z/OS (FMID HPUT110).**
  - sudo for z/OS is supported on z/OS 1.10 and later
  - z/OS 1.10 and z/OS 1.11 requirement: PTF for APAR OA32470 must be applied.
- **Incomplete HOLD ACTION in PTF for APAR OA34949 fix via PE APAR OA37129.**
- **See the "Installing Supplementary Toolkit for z/OS" section in the user's guide for details**

Packaging and installation

- **Pre-installation planning**
  - New directories must be created before installing the APAR.
  - sudo for z/OS requires a GID(0) group to be defined on your system.
  - Ensure file system contains enough available space.
  - Verify the z/OS release requirements noted on the previous slide.
- **See the “Pre-installation planning” section in the user’s guide for details**

Packaging and installation

- **Post-installation setup and verification (Required)**
  - Enable sudo for z/OS - SAMPLIB member HPUTIFA provides an example
  - Copy the sudoers file to /etc/sudoers

```
# sudoers must have mode 0440 (i.e. read for owner and group).
# sudoers must be owned by UID(0) and GID(0).
cp -p /usr/lpp/ported/samples/sudoers /etc/sudoers
```

  - Customize the /etc/sudoers file for your installation using visudo

```
# By default, there's no sudo authority.
# By default, BPXROOT is the default runas and mailto user.
visudo
```

- **See the "Post-installation setup and verification" section in the user's guide for details**

Packaging and installation

- **Post-installation setup and verification (Recommended)**
  - Add a symbolic link to the man pages, if necessary

```
/usr/man/C/man1/hpuza200.book
# symlink --> /usr/lpp/ported/man/C/man1/hpuza200.book
```

  - Add a symbolic link to the message catalog

```
/usr/lib/nls/msg/C/hpusudo.cat
# symlink --> /usr/lpp/ported/lib/nls/msg/C/hpusudo.cat
```

  - Add a symbolic link to the binaries

```
/usr/bin/sudo      # symlink --> /usr/lpp/ported/bin/sudo
/usr/bin/sudoedit  # symlink --> /usr/lpp/ported/bin/sudoedit
/usr/sbin/visudo   # symlink --> /usr/lpp/ported/bin/visudo
```

- **See the “Post-installation setup and verification” section in the user’s guide for details**

Packaging and installation

- **Post-installation setup and verification (Recommended)**
  - Verify sudo for z/OS installation
    - sudo must be owned by UID(0)
    - sudo must have mode 4111 (i.e. execute for all and set-user-ID)
    - sudo must have noshareas extended attribute (i.e. extattr –s)
    - sudo must have the program control extended attribute (i.e. extattr +p)
- **See the "Post-installation setup and verification" section in the user's guide for details**

Packaging and installation

- **Updated toolkit parts for sudo for z/OS**
  - `/usr/lpp/ported/Ported_Tools_License.readme`
  - `/usr/lpp/ported/man/C/man1/hpuza200.book`
  - `SYS1.SAMPLIB(HPUTIFA)`
  - `SYS1.SAMPLIB(HPUTMKDR)`
- **New sudo for z/OS parts**
  - `/usr/lpp/ported/bin/base/sudo-1.7.2p2`
  - `/usr/lpp/ported/bin/base/visudo-1.7.2p2`
  - `/usr/lpp/ported/samples/sudoers`
  - `/usr/lpp/ported/lib/nls/msg/C/hpusudo.cat`
    `# Supporting directories (lib/nls/msg/C) are also new.`

Packaging and installation

- **New sudo for z/OS symbolic links**
  - `/usr/lpp/ported/bin/sudo      # --> base/sudo-1.7.2p2`
  - `/usr/lpp/ported/bin/sudoedit  # --> base/sudoedit-1.7.2p2`
  - `/usr/lpp/ported/bin/visudo    # --> base/visudo-1.7.2p2`
- **New sudo for z/OS hard links**
  - `/usr/lpp/ported/bin/base/sudoedit-1.7.2p2  # --> ./sudo-1.7.2p2`
  - `/usr/lpp/ported/IBM/HPUDXSUD  # --> ../bin/base/sudo-1.7.2p2`
  - `/usr/lpp/ported/IBM/HPUDXVIS  # --> ../bin/base/visudo-1.7.2p2`
  - `/usr/lpp/ported/IBM/HPUDUERS  # --> ../samples/sudoers`
  - `/usr/lpp/ported/IBM/HPUDRCAT  # --> ../lib/nls/msg/C/hpusudo.cat`

Agenda

Overview

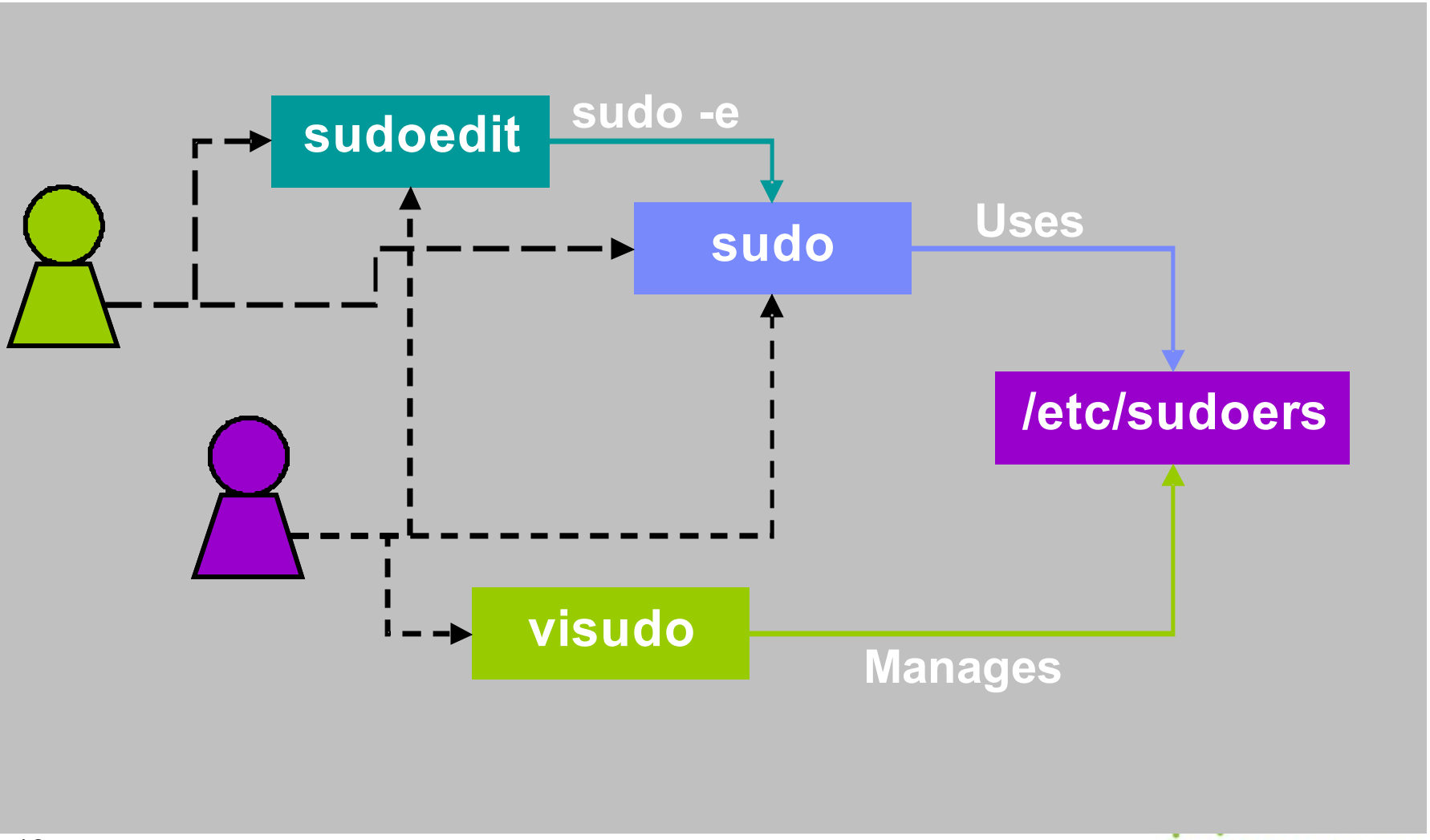
Packaging and installation

>> Usage <<

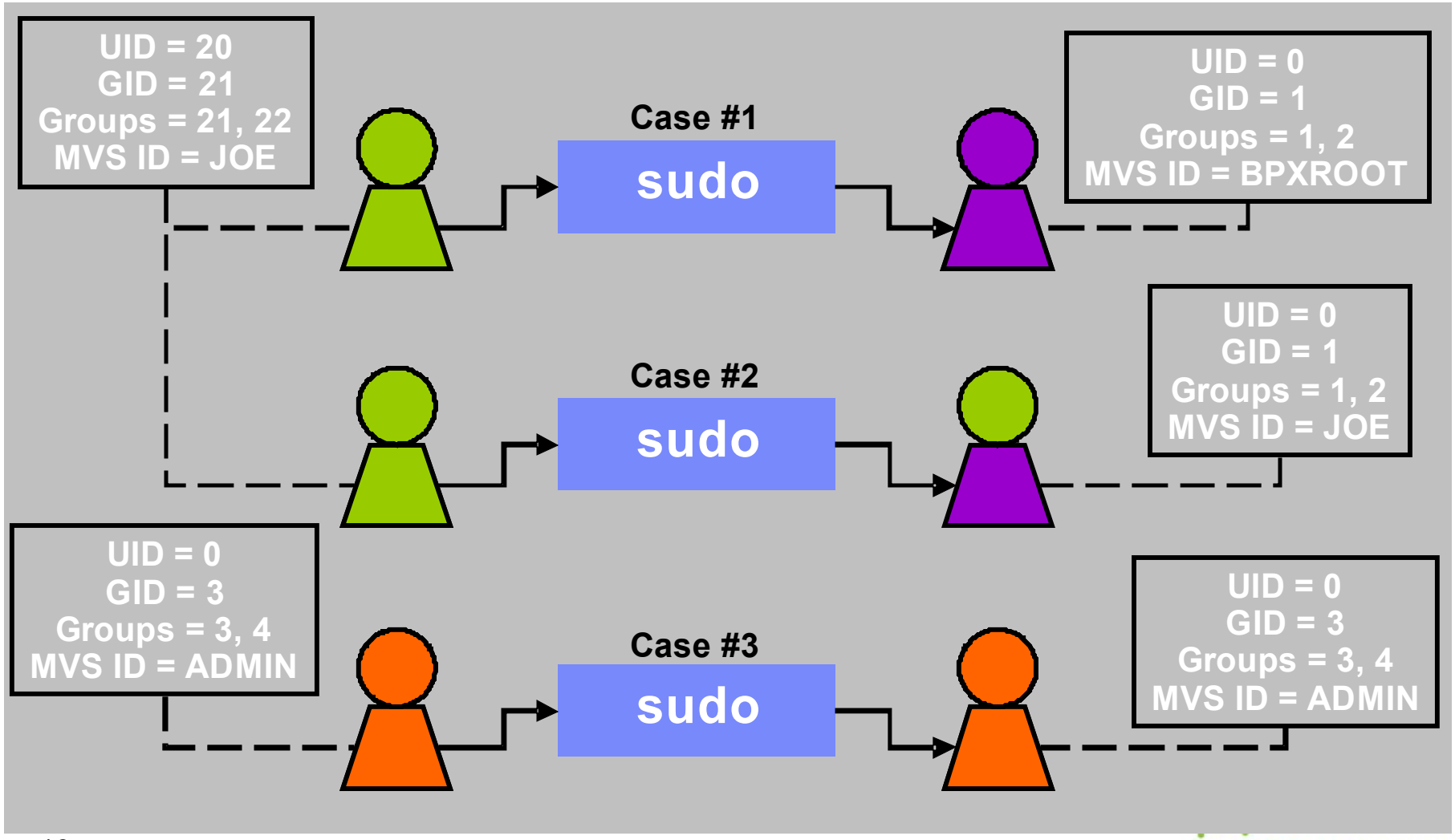
Examples

Appendix

Usage



Usage


UID = 20
GID = 21
Groups = 21, 22
MVS ID = JOE
Case #1
sudo
UID = 0
GID = 1
Groups = 1, 2
MVS ID = BPXROOT
UID = 0
GID = 1
Groups = 1, 2
MVS ID = JOE
Case #2
sudo
UID = 0
GID = 3
Groups = 3, 4
MVS ID = ADMIN
Case #3
sudo
UID = 0
GID = 3
Groups = 3, 4
MVS ID = ADMIN

Usage

Command / Authority	z/OS UNIX ID Change	MVS ID Change	Shell Access	Command Control
sudo	Optional	Optional	Optional	Yes
su <user>	Yes	Yes	Yes	No
su –s <user> (i.e. SURROGAT)	Yes	Yes	Yes	No
su (i.e. BPX.SUPERUSER)	Yes	No	Yes	No
UNIXPRIV	No	No	No	Partial

Usage

- **/etc/sudoers security**
  - Contains sensitive information and must be protected.
  - Must be owned by UID(0) and GID(0) and permissions must be 0440. If not, sudo, sudoedit or visudo will either fix the ownership and permissions or will fail.
  - Only superusers should edit the file (ideally using visudo).
  - Only superusers should be members of the GID(0) group.

Usage

- **/etc/sudoers example**

```
# The sudoers file is composed of two types of entries: aliases (basically
# variables) and user specifications (which specify who may run what).

# The following Defaults specifications are either unique to z/OS or
# have had their default values changed for z/OS.
Defaults !path_info
Defaults ignore_dot
Defaults zos_set_mvs_identity=never

# For better control of which user is selected as the default user,
# the runas_default specification should be set to your desired user.
# You should also set the mailto specification to the desired user.
# The default for both is BPXROOT.
Defaults runas_default=BPXROOT
Defaults mailto=BPXROOT
```

Usage

- **/etc/sudoers example (continued)**

```
# GOOD user specifications:

# Sample user privilege specification to allow a non-UID(0) user (rtheis)
# to edit a UID(0) owned file to which rtheis doesn't have permission.
rtheis ALL= sudoedit /u/root/sharedFiles/file1

# Allow rtheis to display open files for a file system.
rtheis ALL= /bin/fuser -c /tst

# Allow rtheis to run a certain shell script with no arguments.
rtheis ALL= /u/root/script.sh ""
```

Usage

- /etc/sudoers example (continued)

```
# DANGEROUS user specifications:

# Allows shell escapes
# rtheis ALL= /bin/vi /u/root/sharedFiles/file1

# Allows shell access
# rtheis ALL= /bin/sh, /bin/tcsh

# Allows identity chaining
# rtheis ALL= /bin/su, /bin/sudo
```

Usage

- **Security recommendations for user specifications**
  - sudoers grammar (EBNF) can be confusing so use examples
  - Make user specifications as specific as possible
  - Minimize use of the ALL alias and sudo “chaining”
  - Specify commands with arguments or use “” to ensure commands are run without arguments
  - Subtracting commands from the ALL alias using the ‘!’ operator is generally not effective
  - Minimize shell access and shell escapes
- **Suggest reading the user’s guide before using sudo**
  - Specific references: “Preventing shell escapes”, “Security notes” for sudo and “Security notes” for sudoers

Usage

- **Default option value differences between z/OS and open source**
  - sudoers **ignore_dot** option:
    z/OS default = “on”
    open source default = “off”
  - sudoers **runas_default** and **mailto** options:
    z/OS default = “BPXROOT”
    open source default = “root”
  - sudoers **path_info** option:
    z/OS default = “off”
    open source default = “on”

Usage

- **Unsupported open source functionality on z/OS**
  - sudo options: -A askpass, -a type, -c class, -r role, -t type
  - sudoers options: askpass, ignore_local_sudoers, insults, long_opt_prompt, noexec, noexec_file, passprompt_override, pwfeedback, role, rootpw, stay_setuid, sudoers_locale, type, use_loginclass, visiblepw
  - sudoers specifications: netgroup, nonunixgroup, NOEXEC / EXEC

Usage

- **New z/OS-specific functionality**
  - Environment variables: _ZOS_SUDO_NOMSGID and _ZOS_SUDO_DEBUG
  - sudoers options: zos_set_mvs_identity
  - sudoers specifications: ZOS_SET_MVS_IDENTITY / NO_ZOS_SET_MVS_IDENTITY

Caution: Allowing **sudo for z/OS** to change MVS identity means that **su** can be used to do the same!

Agenda

Overview

Packaging and installation

Usage

>> Examples <<

Appendix

Examples

- **Example #1:** Allow users on a team (BACKUPS) the ability to run a specific pax command as a specific UID(0) administrator (admin) with specific arguments determined by the administrator.
  - **/etc/sudoers file entries:**

```
Defaults umask=077
User_Alias BACKUPS = june, fred, mary
BACKUPS ALL = (admin) /bin/pax -x pax -wf /u/code/src.pax /u/code/src
```

  - **sudo command allowed:**

```
sudo –u admin pax -x pax -wf /u/code/src.pax /u/code/src
```

  - **Benefits to using sudo:**
    - Backup team not allowed to view the data they pax'd as an administrator.
    - Backup team not allowed to run other pax commands or change pax options as an administrator.
    - Audit trail provided for every backup done by the backup team.

Examples

- **Example #2:** Log all commands run by UID(0) user.
  - **/etc/sudoers file entries:**
    ```
    admin ALL=(admin) ALL
    ```
  - **sudo command allowed:**
    ```
    sudo rm -rf /u/baduser
    ```
  - **Benefits to using sudo:**
    - Audit trail provided for every command run via sudo by UID(0) user admin.
  - **Example syslog audit entry created by sudo:**
    ```
    Aug 25 08:00:04 SY1 sudo:   admin : TTY=ttyp0000 ;
    PWD=/SYSTEM/tmp/syslogd ; USER=admin ; GROUP=admingrp ;
    COMMAND=/bin/rm -rf /u/baduser
    ```

Agenda

Overview

Packaging and installation

Usage

Examples

>> Appendix <<

Appendix

- **See the updated "IBM Ported Tools for z/OS: Supplementary Toolkit for z/OS Feature User's Guide" for more details on sudo for z/OS.**
  (Order Number: SA23-2234)
- **Website References**
  - IBM Ported Tools for z/OS: http://www.ibm.com/systems/z/os/zos/features/unix/ported/
  - IBM Ported Tools for z/OS: Supplementary Toolkit for z/OS: http://www.ibm.com/systems/z/os/zos/features/unix/ported/suptlk/
  - sudo: http://www.sudo.ws/