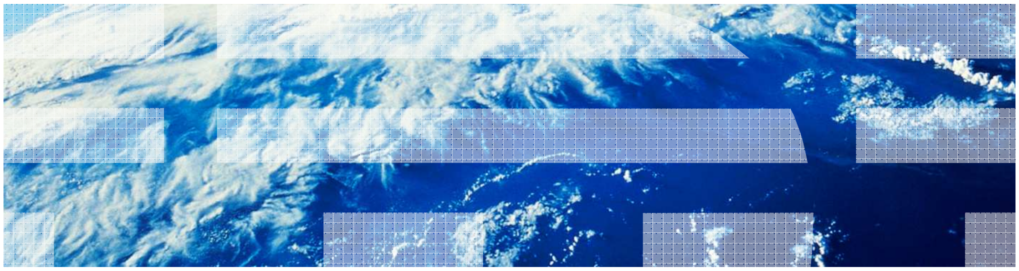
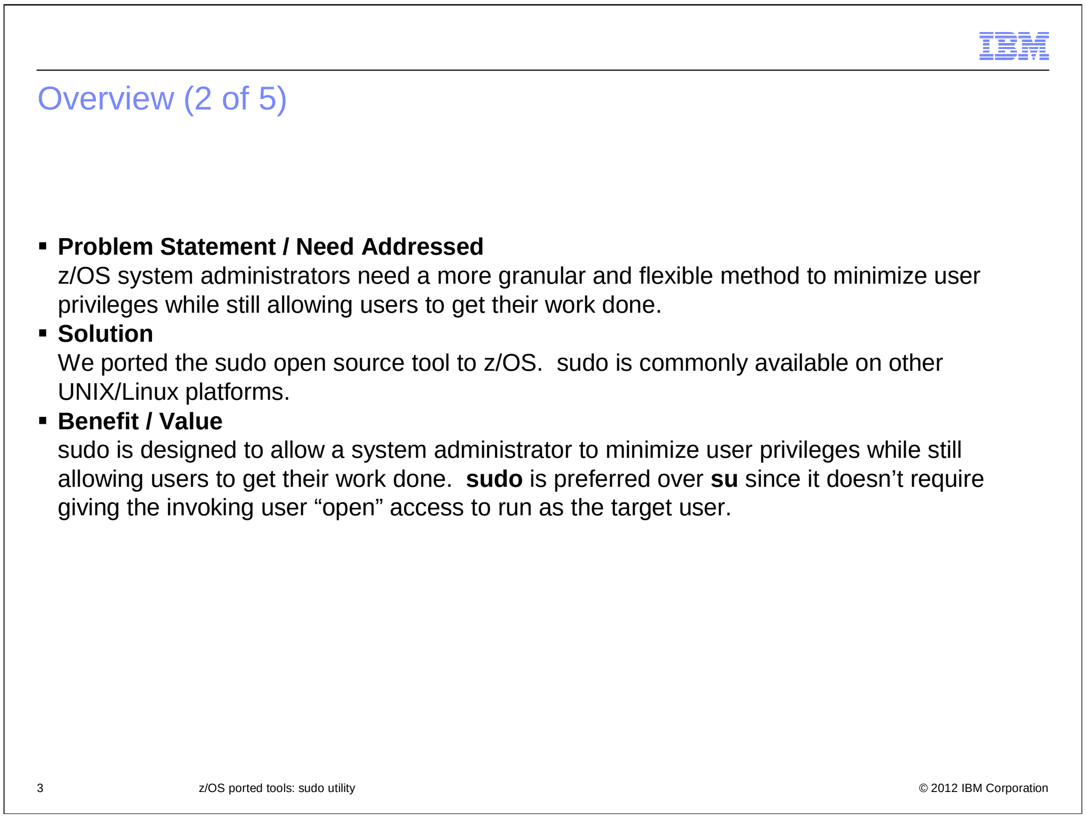
z/OS V1R13

z/OS ported tools: sudo utility



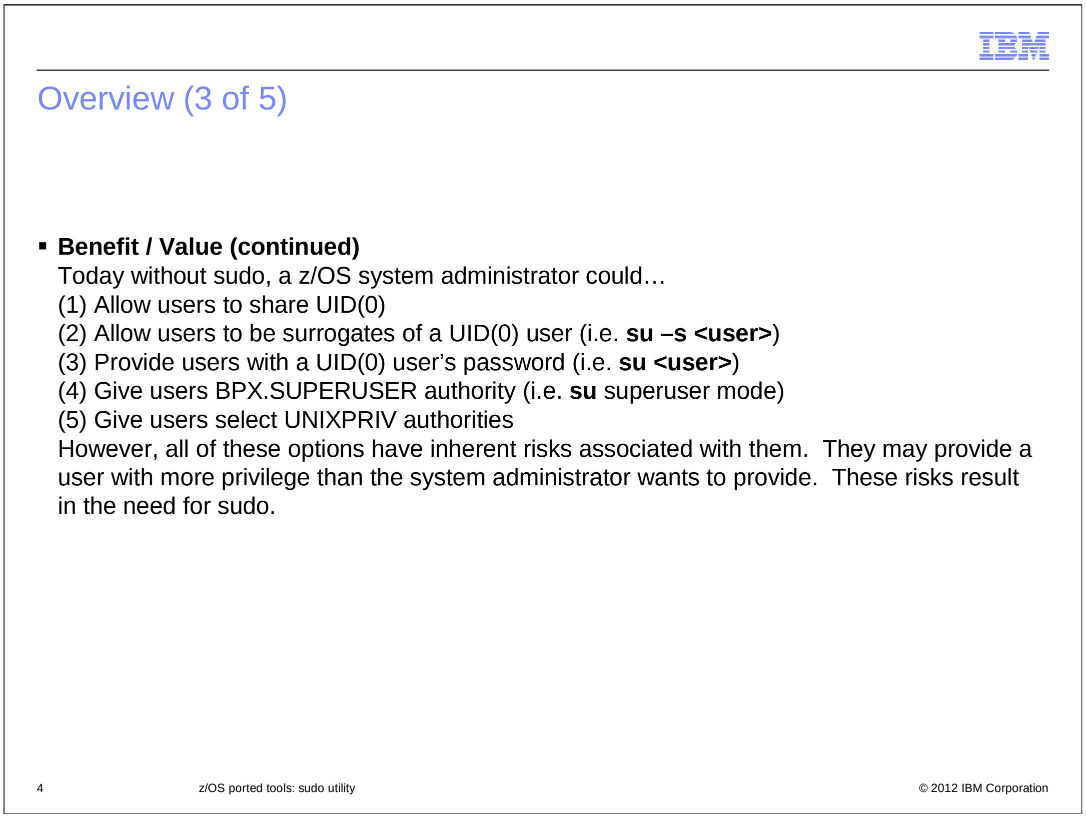
Overview (1 of 5)

- **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 (2 of 5)

- **Problem Statement / Need Addressed**
  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**
  We ported the sudo open source tool to z/OS. sudo is commonly available on other UNIX/Linux platforms.
- **Benefit / Value**
  sudo is designed to allow a system administrator to minimize user privileges while still allowing users to get their work done. **sudo** is preferred over **su** since it doesn't require giving the invoking user "open" access to run as the target user.



Overview (3 of 5)

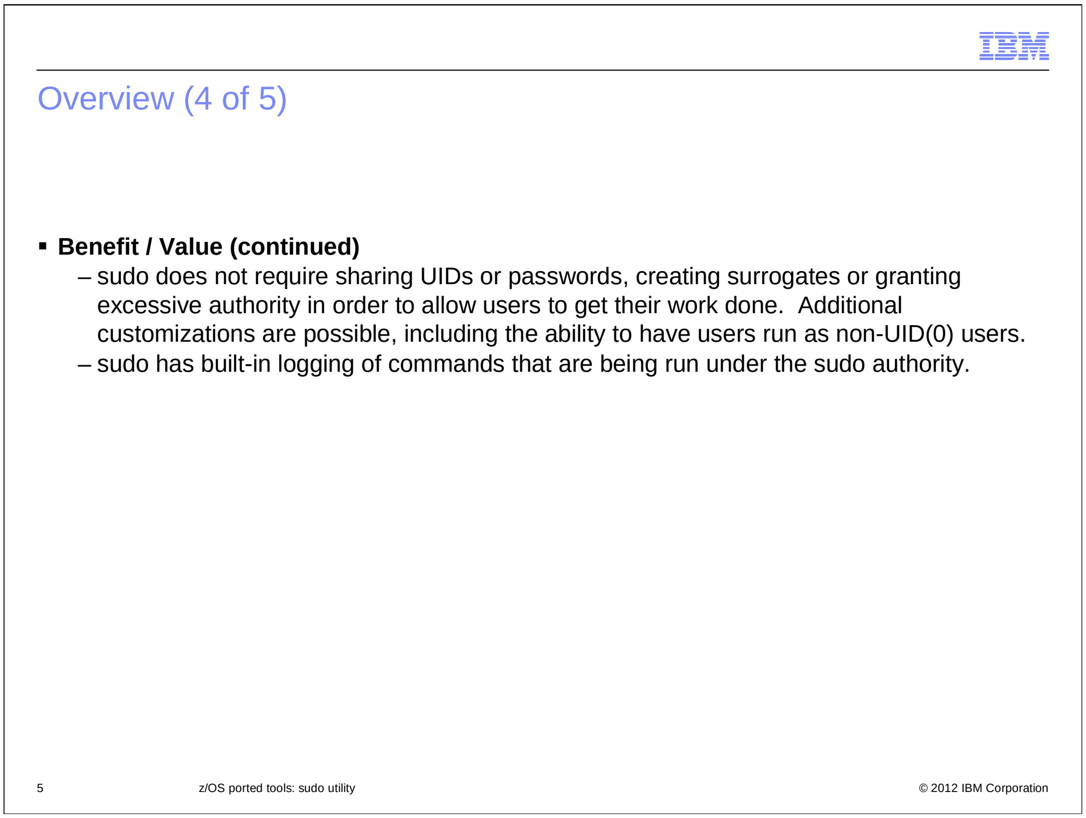
- **Benefit / Value (continued)**
  Today without sudo, a z/OS system administrator could…
  (1) Allow users to share UID(0)
  (2) Allow users to be surrogates of a UID(0) user (i.e. **su –s <user>**)
  (3) Provide users with a UID(0) user's password (i.e. **su <user>**)
  (4) Give users BPX.SUPERUSER 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.

4 z/OS ported tools: sudo utility

(1), (2) and (3) allow an invoking user to obtain a UID(0) user's UID, GID, Groups and MVS identity.

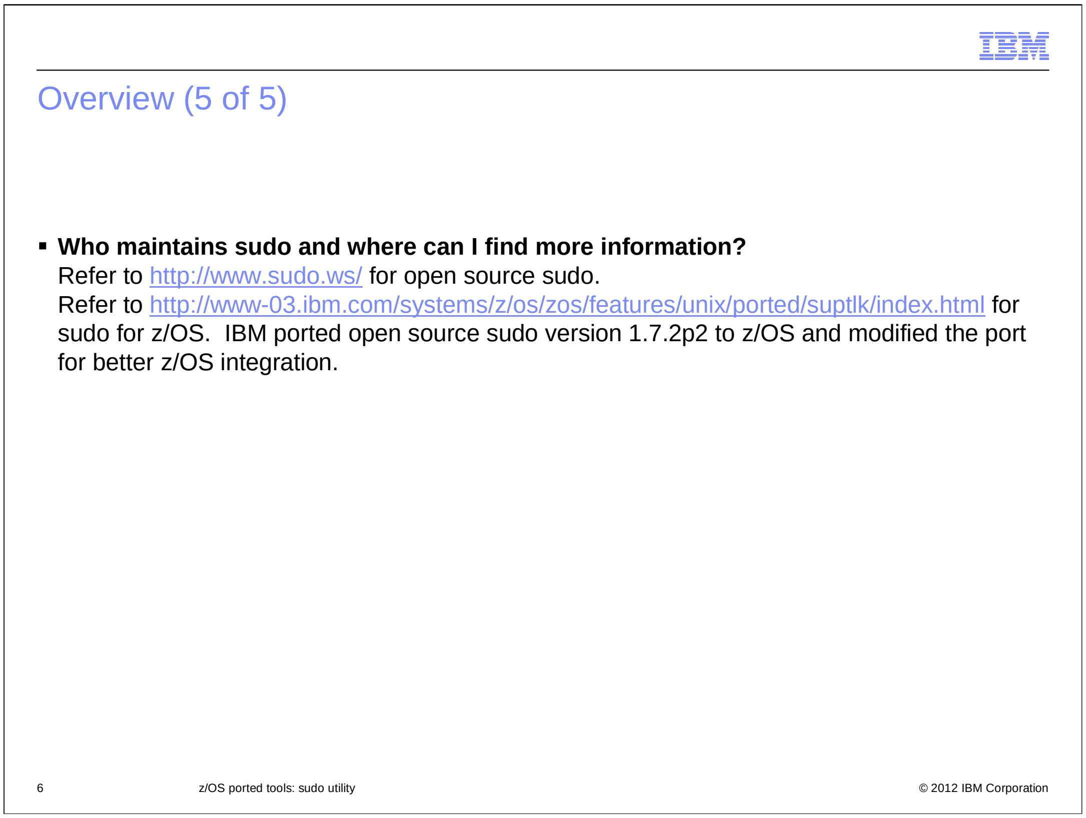
(4) allows an invoking user to obtain a UID(0) user's UID, GID, Groups. However, the invoking user's MVS identity is NOT changed.

(5) doesn't change a user's z/OS UNIX or MVS identities. Rather, the user is given authority to perform certain operations (e.g. mount).



Overview (4 of 5)

- **Benefit / Value (continued)**
  - sudo does not 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 has built-in logging of commands that are being run under the sudo authority.



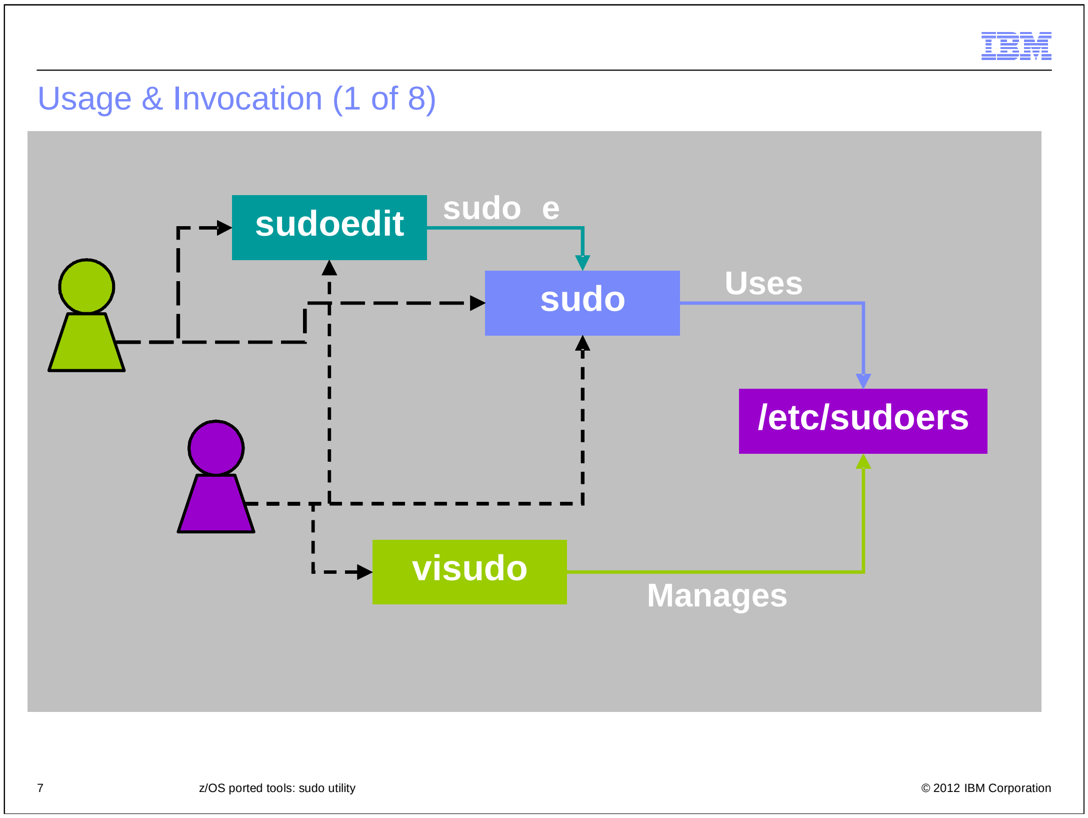
Overview (5 of 5)

- **Who maintains sudo and where can I find more information?**
  Refer to http://www.sudo.ws/ for open source sudo.
  Refer to http://www-03.ibm.com/systems/z/os/zos/features/unix/ported/suptlk/index.html for sudo for z/OS. IBM ported open source sudo version 1.7.2p2 to z/OS and modified the port for better z/OS integration.

FITS Requirements Addressed:

• MR0402036647 - Provide "sudo" command in z/OS USS shell

• MR08024061647 - Provide "sudo" command in z/OS USS shell



Usage & Invocation (1 of 8)

sudoedit

sudo e

sudo

Uses

/etc/sudoers

visudo

Manages

7 z/OS ported tools: sudo utility © 2012 IBM Corporation

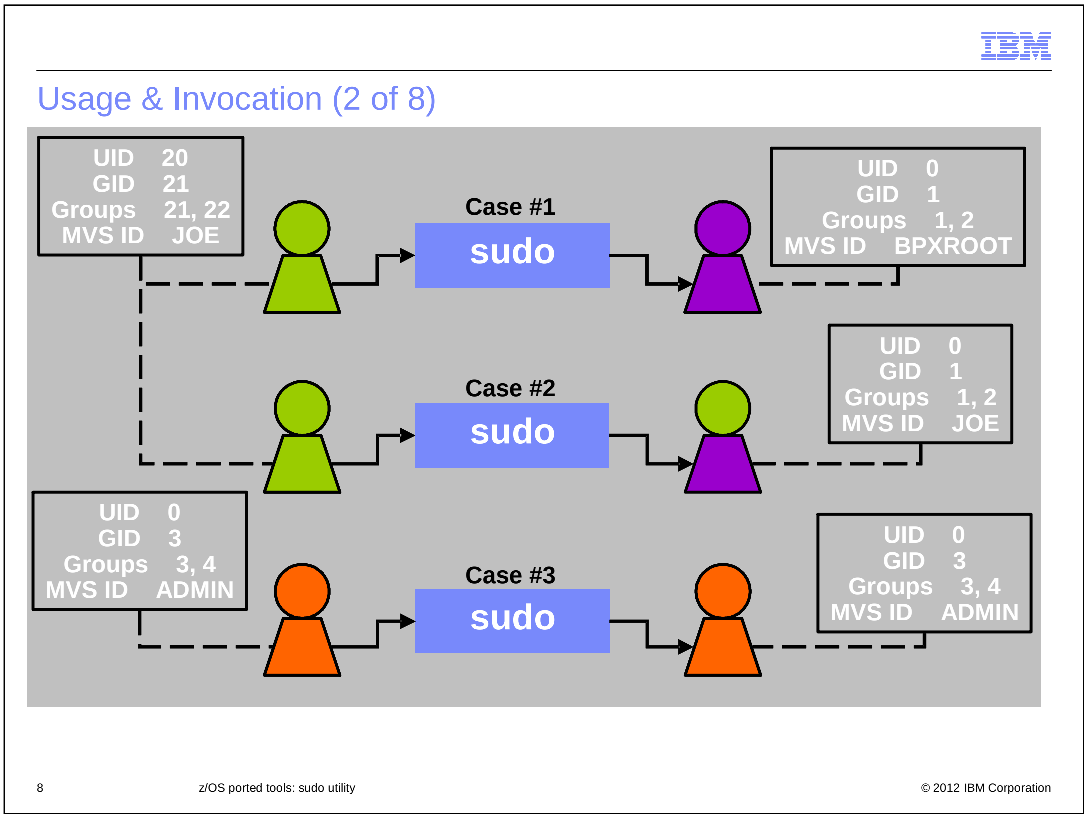
sudo allows a permitted user to execute a command as a superuser (UID(0)) or another user, as specified in the sudoers file. The real and effective UID and GID are set to match those of the target user as specified in the user database and the group vector is initialized based on the group file (unless the **-P** option was specified). The MVS identity may also be changed to correspond to the target user. There are additional authority requirements unique to z/OS that must be met to change the MVS identity. See the sudoers **zos_set_mvs_identity** option for more information.

sudoedit is the same as running **sudo** with the –e option.

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

visudo edits the sudoers file in a safe fashion. **visudo** locks the sudoers file against multiple simultaneous edits, provides basic sanity checks, and checks for parse errors. If the sudoers file is currently being edited, you will receive a message to try again later.

By default, all users are allowed to “attempt” to use **sudo** or **sudoedit**, however, only UID(0) users are allowed to use **visudo** and manage the /etc/sudoers file.



Usage & Invocation (2 of 8)

UID 20
GID 21
Groups 21, 22
MVS ID JOE

Case #1

sudo

UID 0
GID 1
Groups 1, 2
MVS ID BPXROOT

Case #2

sudo

UID 0
GID 1
Groups 1, 2
MVS ID JOE

UID 0
GID 3
Groups 3, 4
MVS ID ADMIN

Case #3

sudo

UID 0
GID 3
Groups 3, 4
MVS ID ADMIN

8 z/OS ported tools: sudo utility © 2012 IBM Corporation

sudo sets the real and effective UID and GID to match those of the target user as specified in the user database and the group vector is initialized based on the group file (unless the **-P** option was specified). The MVS identity may also be changed to correspond to the target user. There are additional authority requirements unique to z/OS that must be met to change the MVS identity. See the sudoers **zos_set_mvs_identity** option for more information

Case #1 (Full identity change):

User JOE uses sudo to run fully as user BPXROOT. This is how the su command works when a user is specified.

Case #2 (Partial identity change – default behavior):

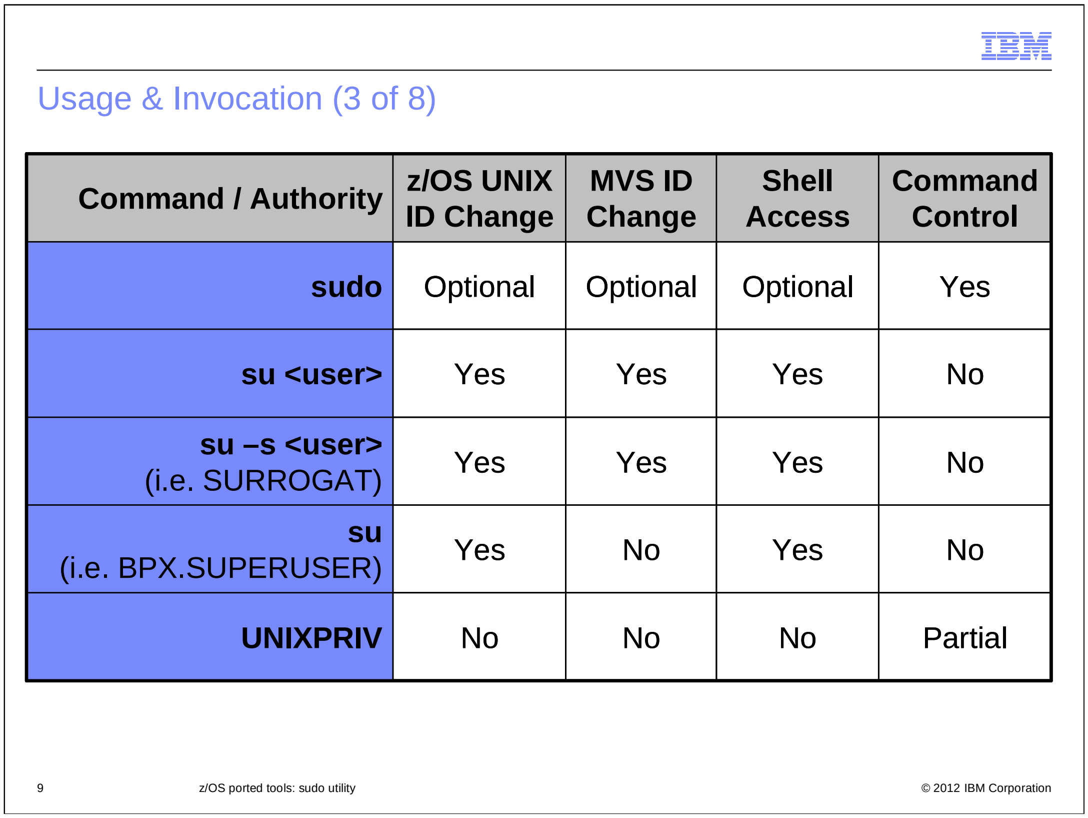
User JOE uses sudo to run partially as user BPXROOT. That is, JOE has BPXROOT’s z/OS UNIX identity (i.e. UID, GID and groups) however, JOE doesn’t get BPXROOT’s MVS identity. This how the su command works for a BPX.SUPERUSER switch.

Case #3 (No identity change - use sudo for auditing):

User ADMIN uses sudo to run fully as user ADMIN. This is often used by system administrators would like an easy way to log the commands and arguments used on commands that they run themselves as UID(0) users. sudo can be used to do this (and often is on other UNIX platforms).

Other Cases:

There are other not-as-common “runas” cases for sudo that aren’t highlighted on this slide. Refer to the user’s guide for details.

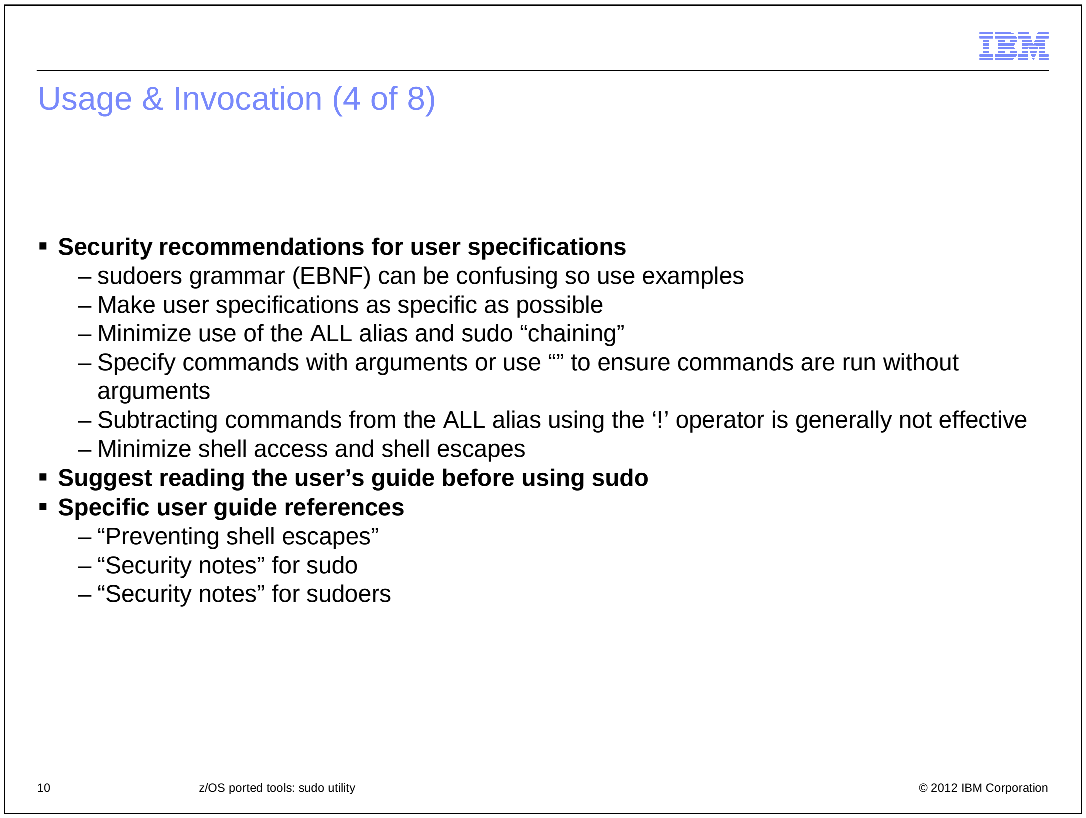


Usage & Invocation (3 of 8)

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

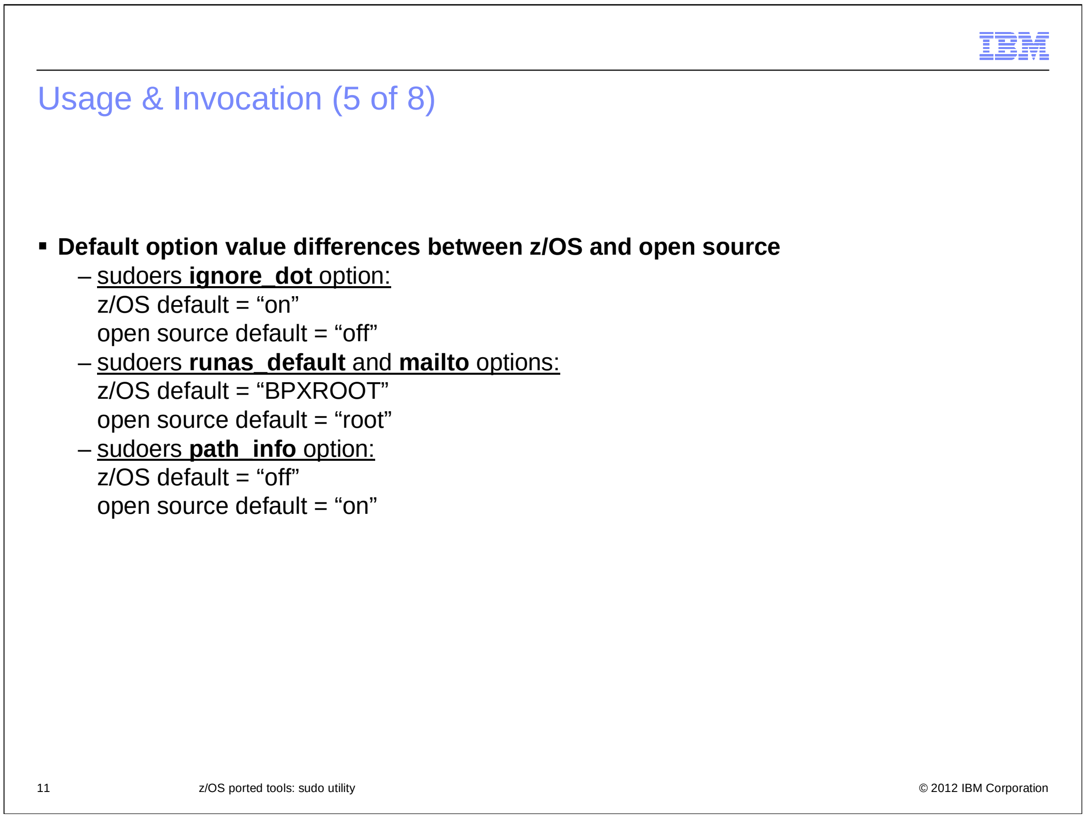
The table compares the authority change and actions allowed/denied for various authority modifying mechanisms on z/OS.

“Command Control” refers to the ability to control the commands (and their arguments) run by a user after an ID change.



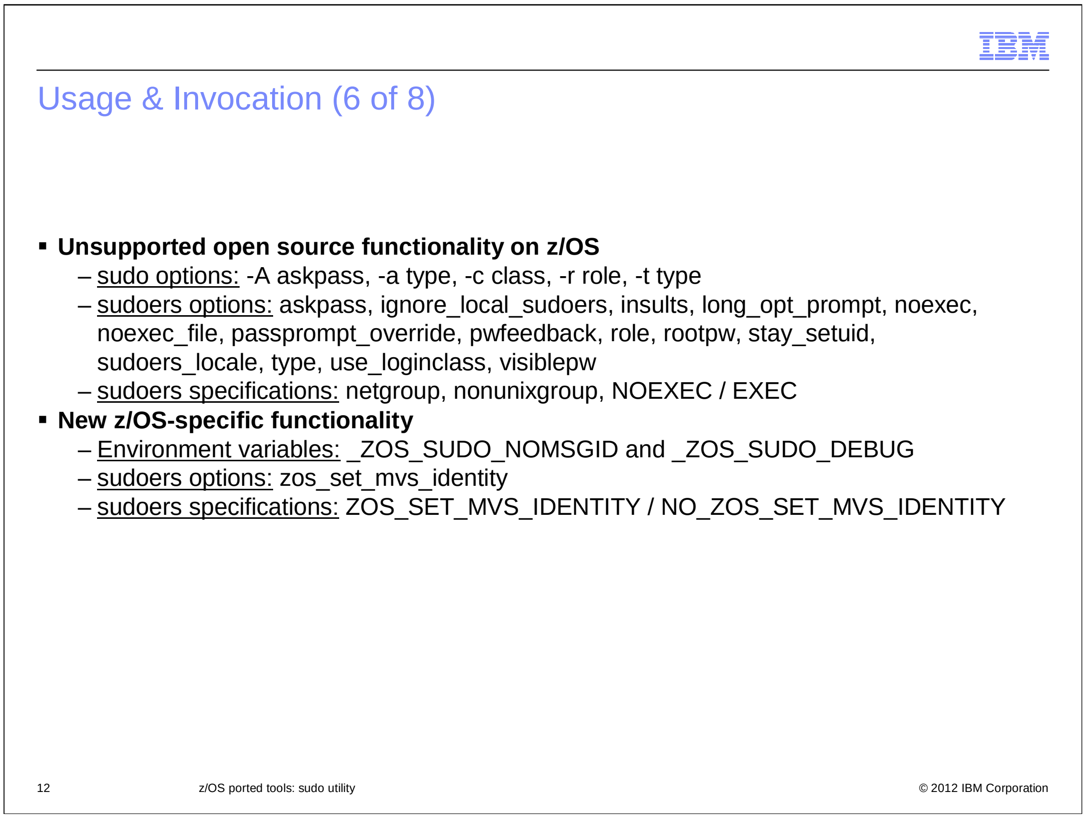
Usage & Invocation (4 of 8)

- **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 user guide references**
  - “Preventing shell escapes”
  - “Security notes” for sudo
  - “Security notes” for sudoers



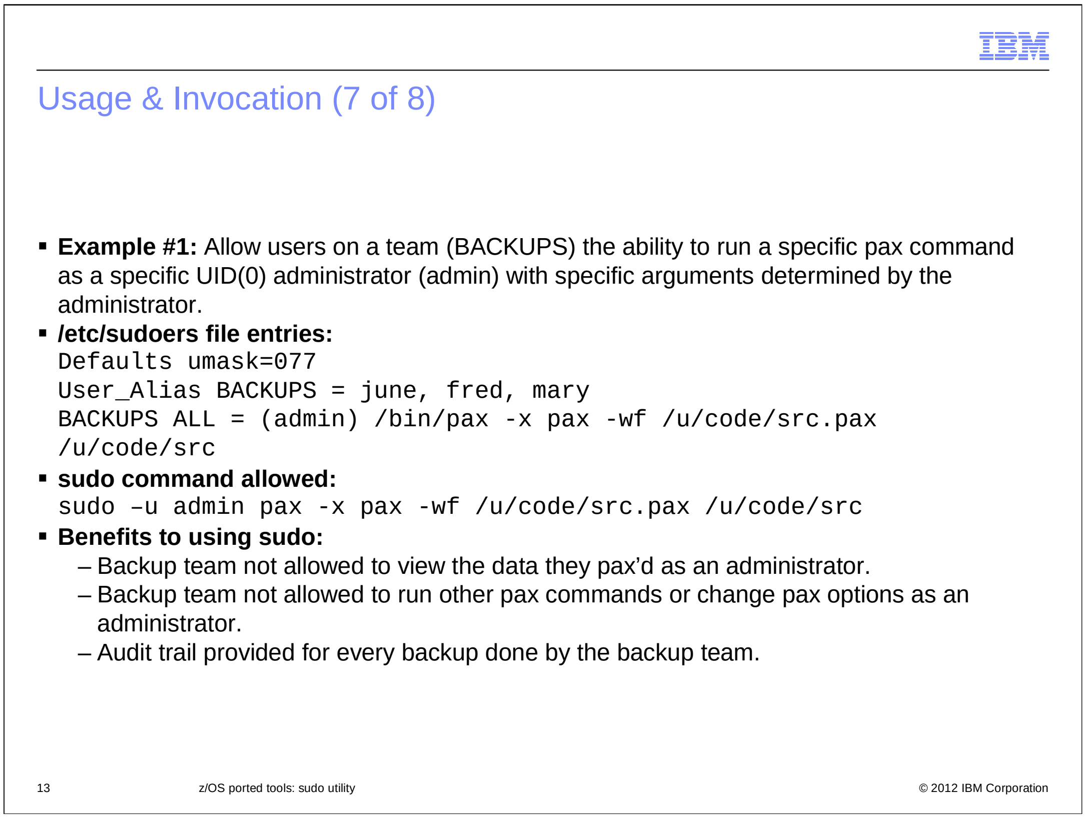
Usage & Invocation (5 of 8)

- **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 & Invocation (6 of 8)

- **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
- **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



Usage & Invocation (7 of 8)

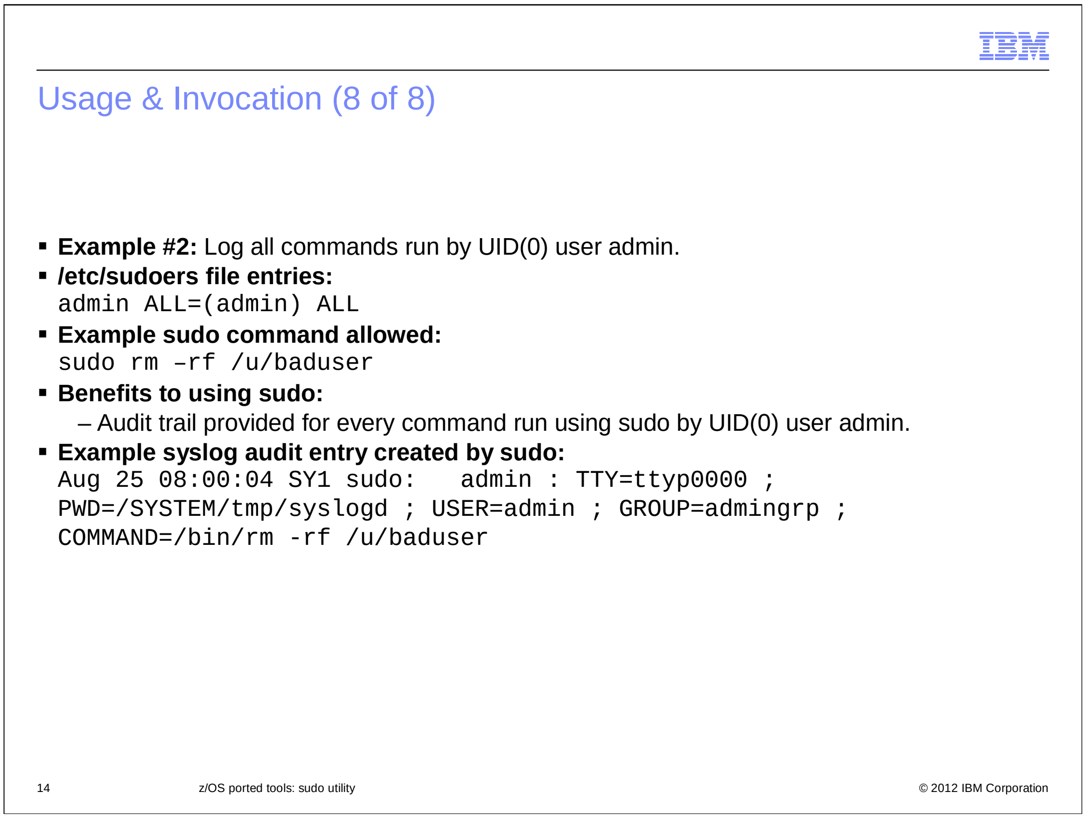
- **Example #1:** Allow users on a team (BACKUPS) the ability to run a specific pax command as a specific UID(0) administrator (admin) with specific arguments determined by the administrator.
- **/etc/sudoers file entries:**

```
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.



Usage & Invocation (8 of 8)

- **Example #2:** Log all commands run by UID(0) user admin.
- **/etc/sudoers file entries:**

```
admin ALL=(admin) ALL
```

- **Example sudo command allowed:**

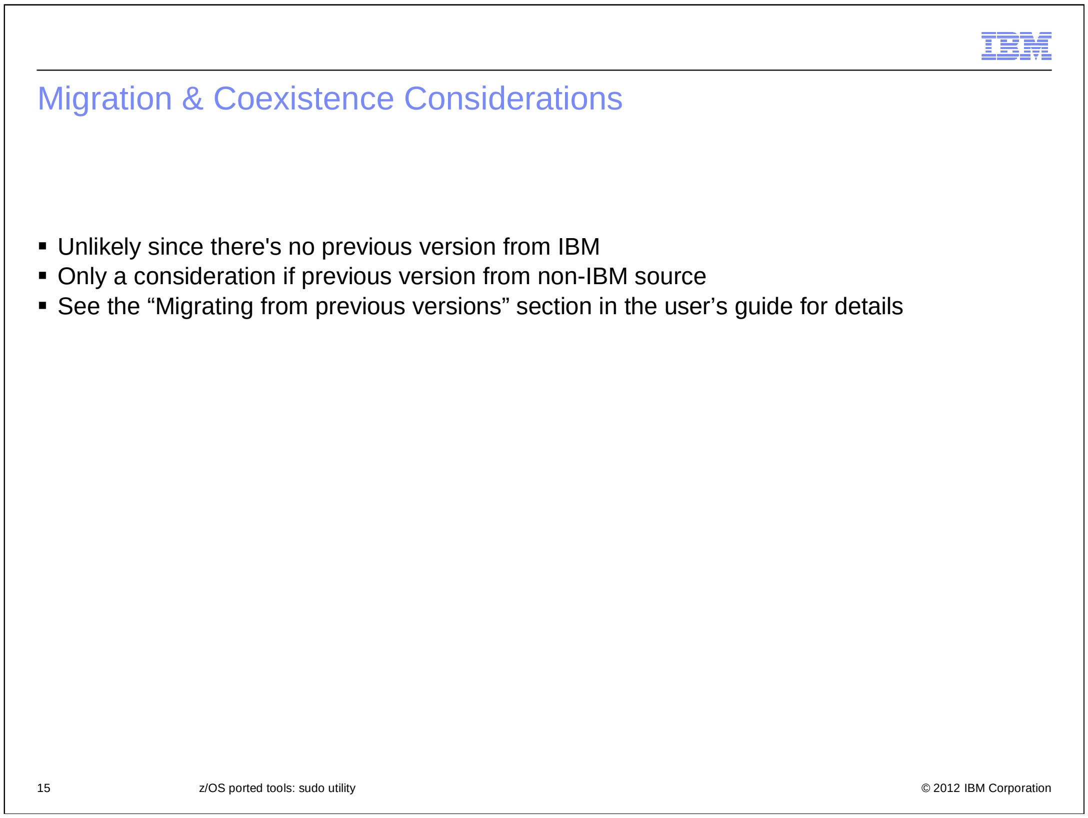
```
sudo rm –rf /u/baduser
```

- **Benefits to using sudo:**
  - Audit trail provided for every command run using 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
```

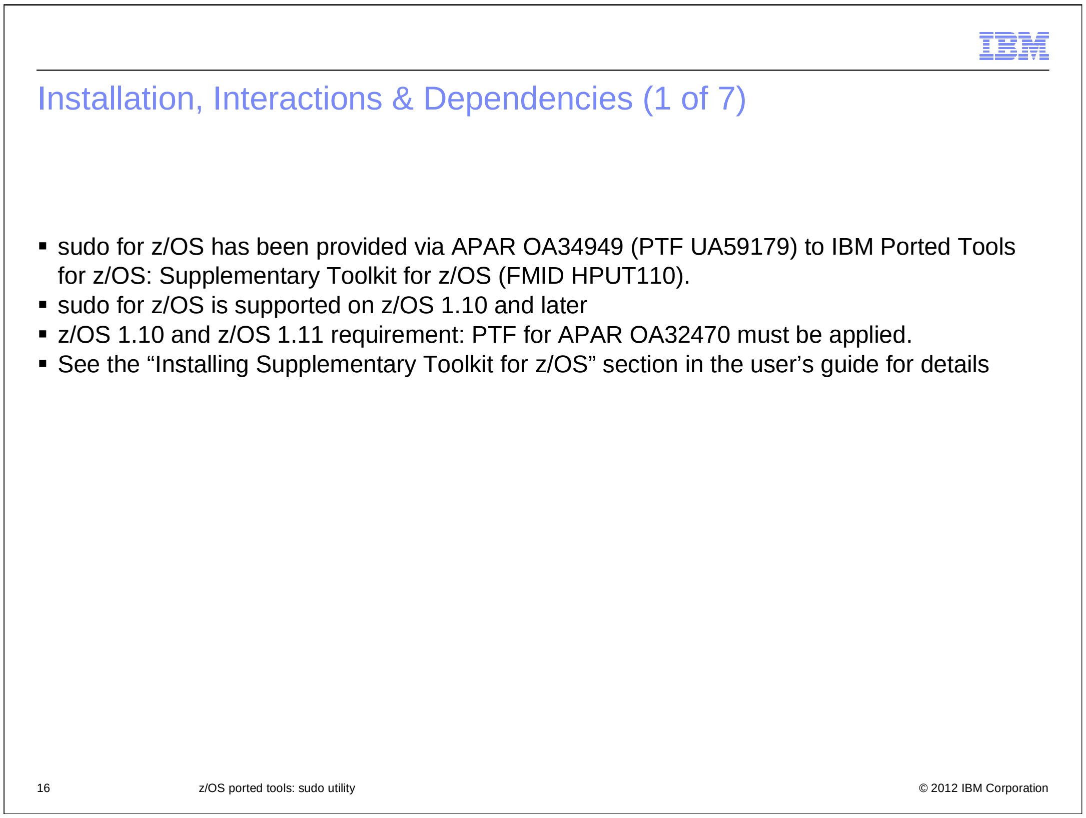
14 z/OS ported tools: sudo utility © 2012 IBM Corporation

sudo can log both successful and unsuccessful attempts (as well as errors) to syslog, a log file, or both. By default, **sudo** will log by way of syslog, but this is changeable by way of the **sudoers** file.



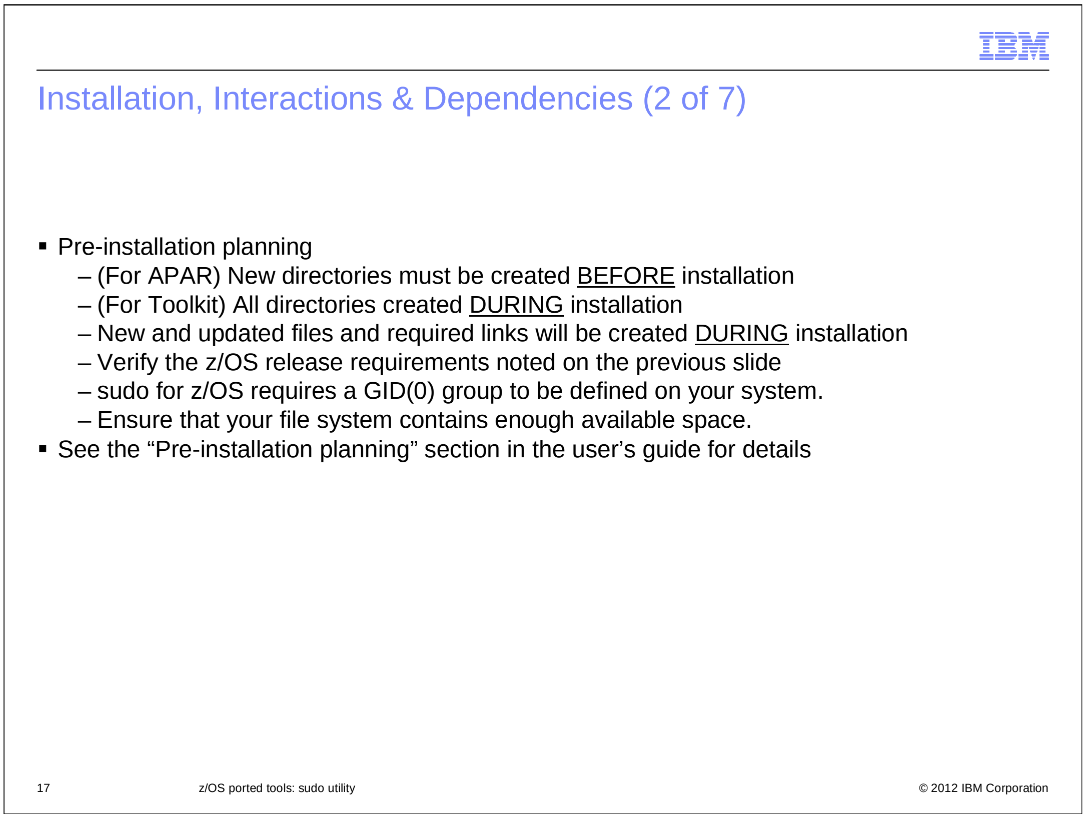
Migration & Coexistence Considerations

- Unlikely since there's no previous version from IBM
- Only a consideration if previous version from non-IBM source
- See the “Migrating from previous versions” section in the user’s guide for details



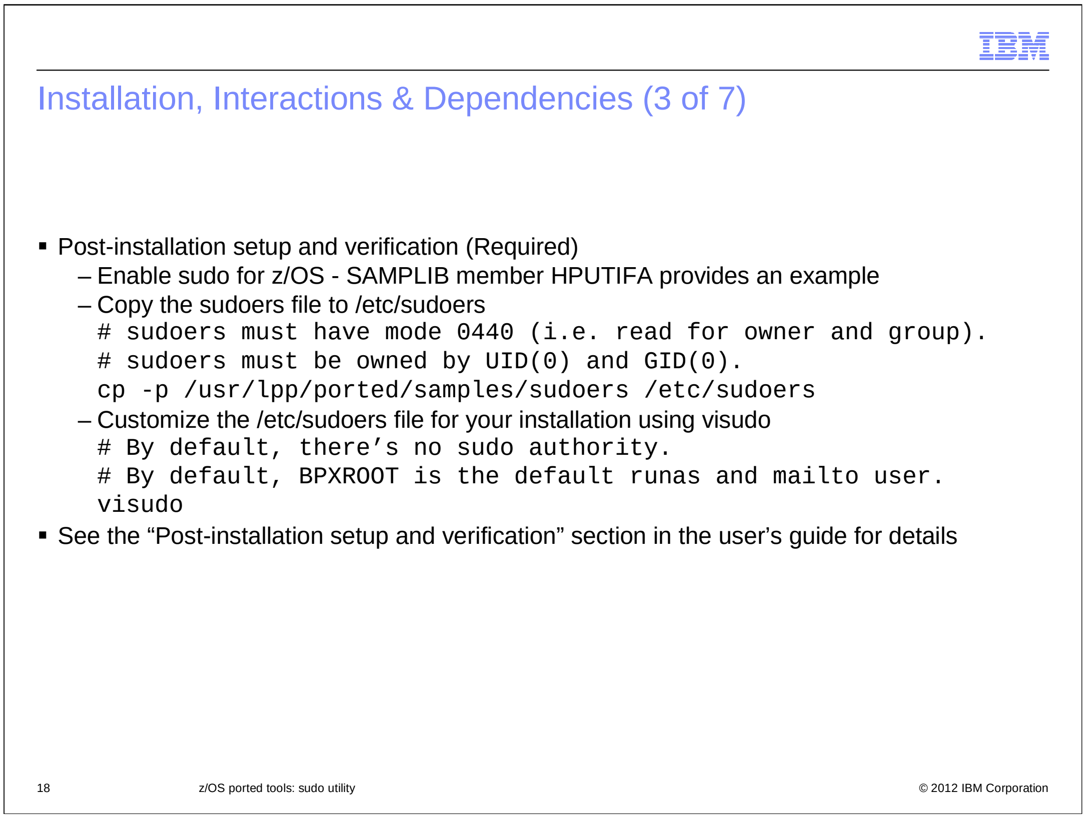
Installation, Interactions & Dependencies (1 of 7)

- 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.
- See the “Installing Supplementary Toolkit for z/OS” section in the user’s guide for details



Installation, Interactions & Dependencies (2 of 7)

- Pre-installation planning
  - (For APAR) New directories must be created BEFORE installation
  - (For Toolkit) All directories created DURING installation
  - New and updated files and required links will be created DURING installation
  - Verify the z/OS release requirements noted on the previous slide
  - sudo for z/OS requires a GID(0) group to be defined on your system.
  - Ensure that your file system contains enough available space.
- See the “Pre-installation planning” section in the user’s guide for details

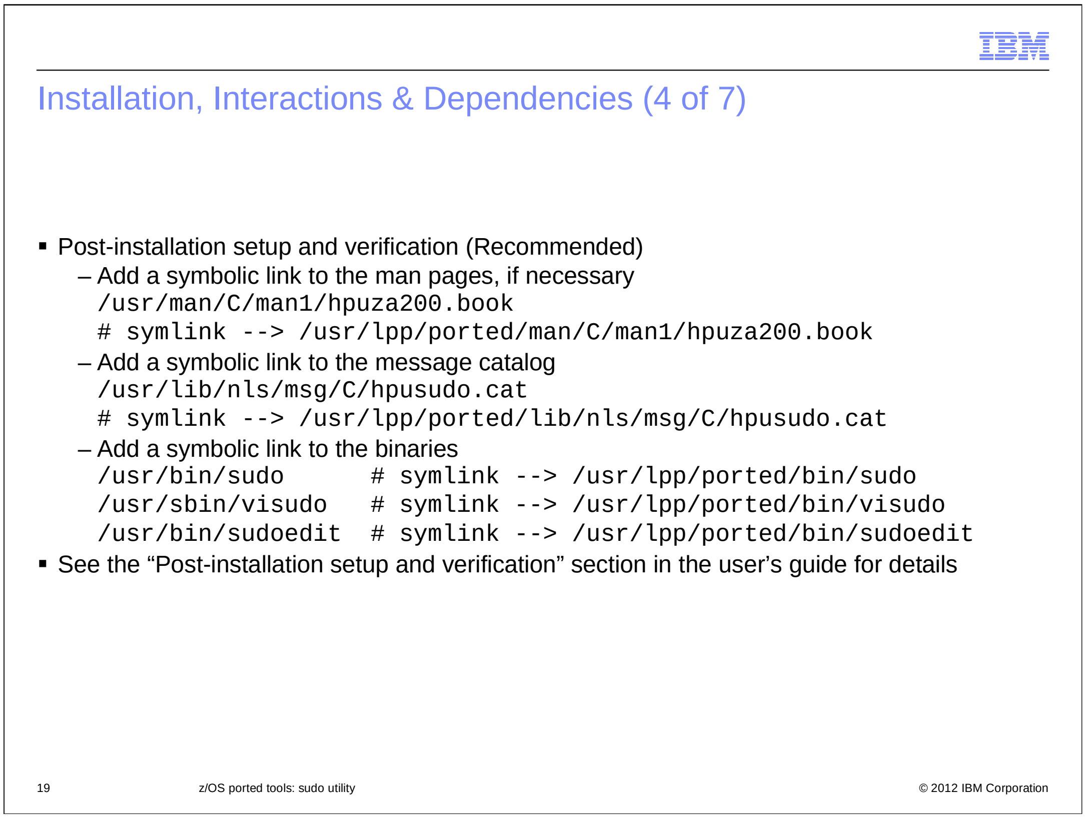


Installation, Interactions & Dependencies (3 of 7)

- 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



Installation, Interactions & Dependencies (4 of 7)

- 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
    ```

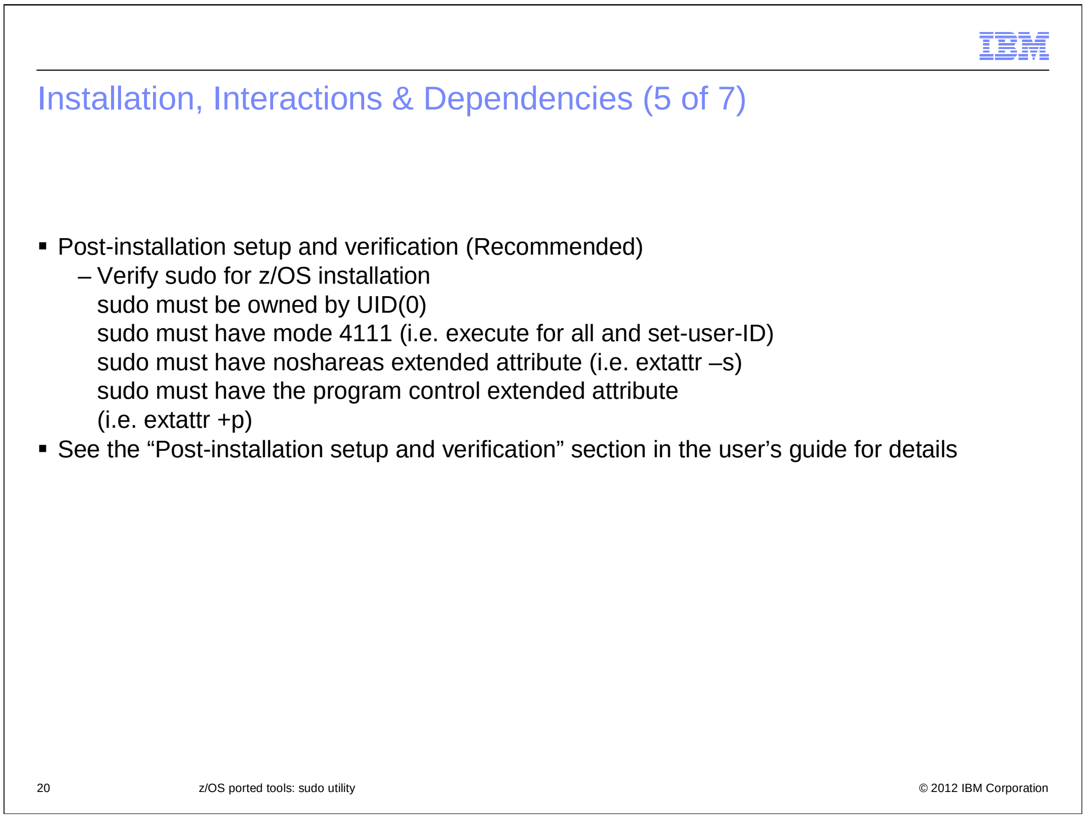
  - Add a symbolic link to the message catalog

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

  - Add a symbolic link to the binaries

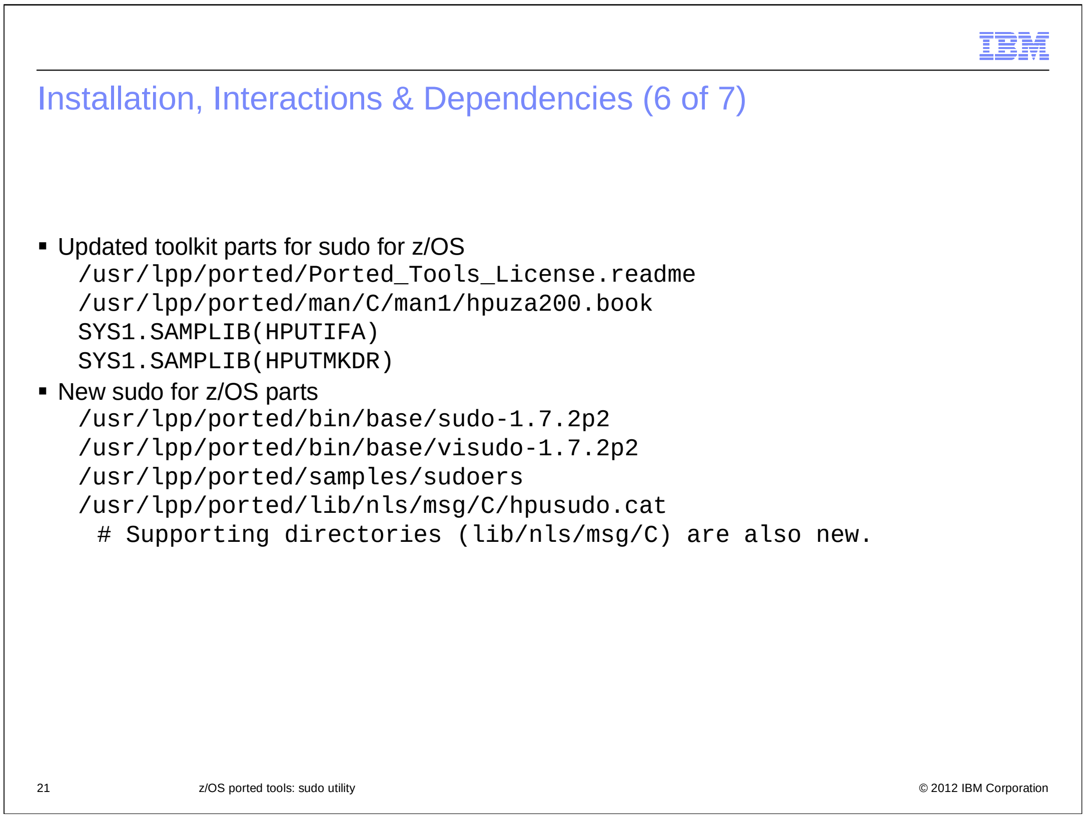
    ```
    /usr/bin/sudo      # symlink --> /usr/lpp/ported/bin/sudo
    /usr/sbin/visudo   # symlink --> /usr/lpp/ported/bin/visudo
    /usr/bin/sudoedit  # symlink --> /usr/lpp/ported/bin/sudoedit
    ```

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



Installation, Interactions & Dependencies (5 of 7)

- 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



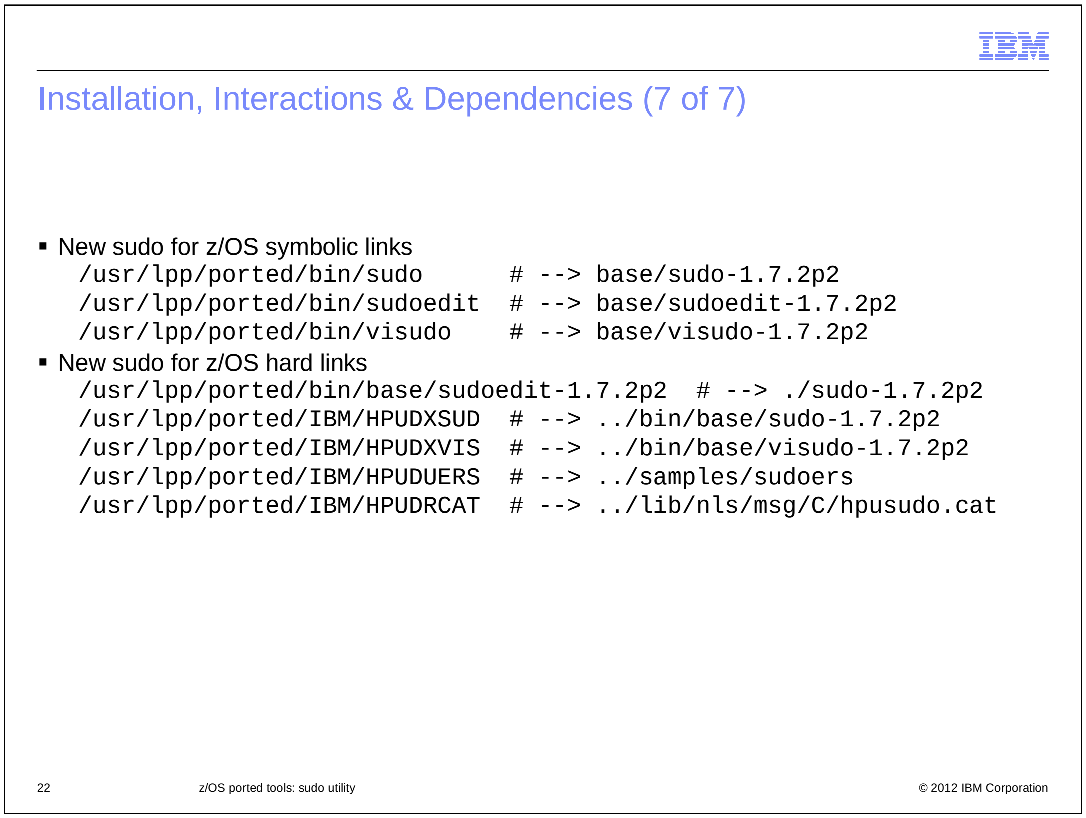
Installation, Interactions & Dependencies (6 of 7)

- 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.
```



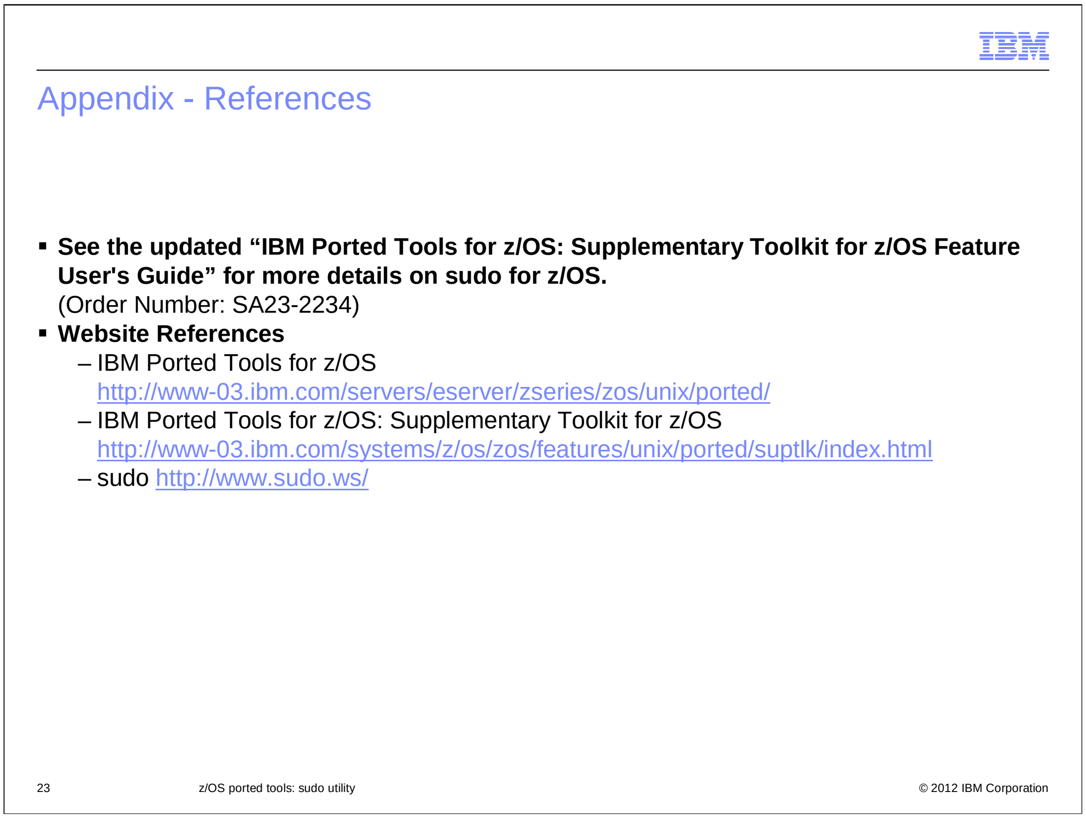
Installation, Interactions & Dependencies (7 of 7)

- 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
```

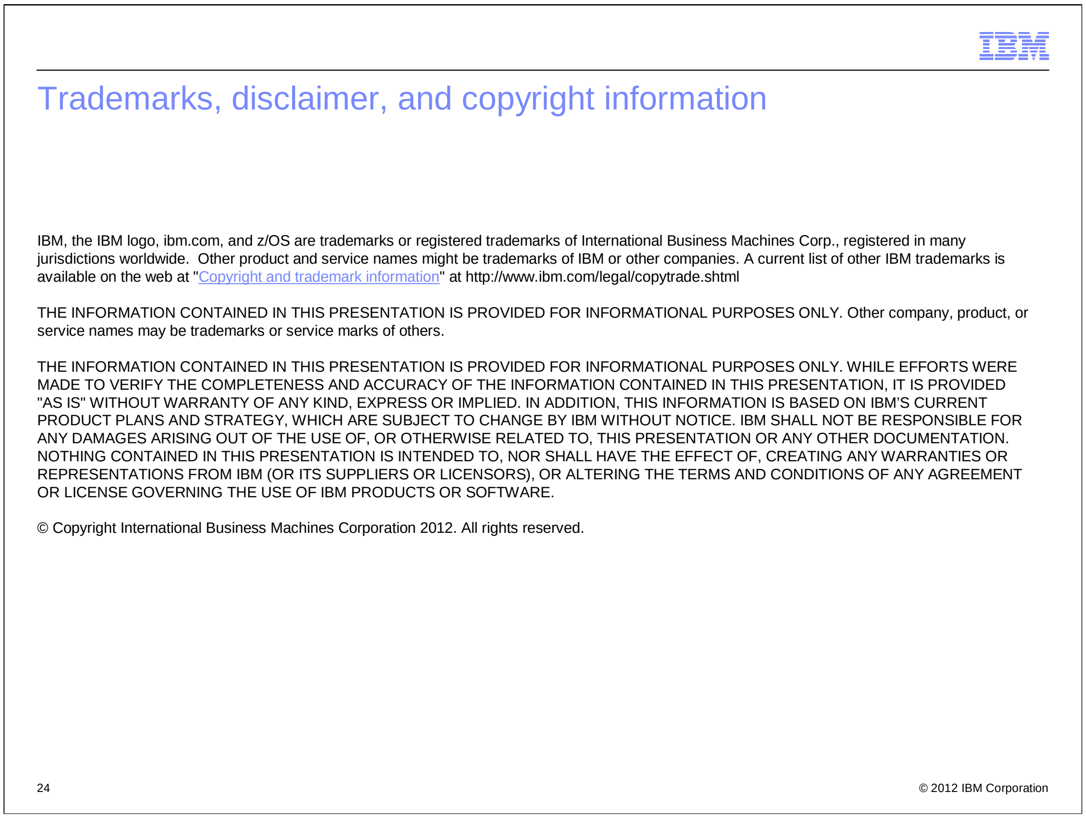
- New sudo for z/OS hard links

```
/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
```



Appendix - References

- **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-03.ibm.com/servers/eserver/zseries/zos/unix/ported/
  - IBM Ported Tools for z/OS: Supplementary Toolkit for z/OS
    http://www-03.ibm.com/systems/z/os/zos/features/unix/ported/suptlk/index.html
  - sudo http://www.sudo.ws/



Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. Other company, product, or service names may be trademarks or service marks of others.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.