SAP NetWeaver 2004s SPS 4

Security Guide

SAP System Security Under UNIX/LINUX

Document Version 1.00 – October 24, 2005

SAP AG
Neurottstraße 16
69190 Walldorf
Germany
T +49/18 05/34 34 24
F +49/18 05/34 34 20
www.sap.com

Disclaimer

Some components of this product are based on Java™. Any code change in these components may cause unpredictable and severe malfunctions and is therefore expressively prohibited, as is any decompilation of these components.

Any Java™ Source Code delivered with this product is only to be used by SAP's Support Services and may not be modified or altered in any way.

Documentation in the SAP Service Marketplace

You can find this documentation at the following Internet address:
`service.sap.com/securityguide`

Typographic Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation
Example text	Emphasized words or phrases in body text, graphic titles, and table titles
EXAMPLE TEXT	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example text`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, *F2* or *ENTER*.

Icons

Icon	Meaning
	Caution
	Example
	Note
	Recommendation
	Syntax

Additional icons are used in SAP Library documentation to help you identify different types of information at a glance. For more information, see *Help on Help → General Information Classes and Information Classes for Business Information Warehouse* on the first page of any version of *SAP Library*.

Contents

SAP System Security Under UNIX/LINUX 5
1 Securing the Base Installation.....5
2 Protecting Specific Properties, Files and Services 6
3 Protected SAP System Directory Structures Under UNIX/LINUX...8
4 Setting Access Privileges for SAP System Directories Under UNIX/LINUX.....9
5 Setting Rights for an Installation with Several SAP Systems 10
6 Additional Information on UNIX/LINUX Security.....10

SAP System Security Under UNIX/LINUX

In the following topics, we cover the aspects pertaining to security under the UNIX or LINUX operating systems. When appropriate, we include our recommendations and any measures that you need to take.

- Protecting Specific Properties, Files and Services [Page 6]
- Protected SAP System Directory Structures Under UNIX/LINUX [Page 8]
- Setting Access Privileges for SAP System Directories Under UNIX/LINUX [Page 9]
- Additional Information on UNIX/LINUX Security [Page 10]

The most important recommendation for securing your system at the operating system level is to **keep your operating system up to date!** Stay informed and install any security-related patches that are released by your operating system vendor.

1 Securing the Base Installation

Because the security level for a newly installed UNIX or LINUX operating system does not likely suffice to meet your security requirements, we recommend taking the following precautions after the installation:

- **Harden the operating system**

  After the initial installation of the UNIX or LINUX operating system, you should “harden” the system to remove any unnecessary services and set the rights for operating system resources that may not be sufficiently protected.

  Most of the UNIX and LINUX vendors provide scripts and directions for hardening their systems. Therefore, for more information, refer to your operating system vendor.

- **Check the integrity of system files on a regular basis**

  Because changes to system files are not necessarily detected by the operating system, we recommend checking the integrity of such files on a regular basis. Check with your operating system vendor for available tools and guidelines.

- **Restrict access to the operating system**

  System access should be restricted to authorized users only. In addition, all logons should be logged and monitored so that you can track user activities. For more information about how log and monitor logons, see the documentation provided by your operating system vendor.

- **Restrict physical access to the server**

  To prevent users from being able to misuse certain functions, for example, modifying boot processes, you should restrict physical access to the server. Such functions should only be available locally, and only authorized administrators should have physical access to the server. You should also have such administration activities logged.

- **Protect access to the server at the network level**

  You should also protect access to the server at the network level. Use a firewall system to allow access only over those ports that are necessary. For more information, see Network and Communication Security [SAP Library].

2 Protecting Specific Properties, Files and Services

There are certain precautions to take when using any of the following properties, files or services:

- **SUID/SGID programs**

  The SUID/SGID property gives programs extended privileges that exceed the privileges possessed by the caller.

  Every UNIX system contains a large number of these programs for administrative purposes. These programs may contain known errors that unauthorized users may be able to take advantage of in order to assign new access rights to themselves.

  For example, the `SENDMAIL` program is such a SUID program. We suggest that you only use versions of `SENDMAIL` (or similar SUID programs) in which known errors have been corrected.

- **Password file (`passwd`)**

  Although UNIX hashes passwords before storing them in this file, a user could use a dictionary-attack program to discover password information contained in this file.

  You can improve security by using a shadow password file that allows only the user `root` to access the password information.

- **BSD services `rlogin` and `remsh/rsh`,**

  These services permit remote access to UNIX machines. At logon, the files `/etc/host.equiv` and `$HOME/.rhosts` are checked. If either of these files contains the hostname or the IP address of the connection originator or a wildcard character (+), then the user can log on without having to supply a password.

  You should be aware that the UNIX services for `rlogin` and `remsh/rsh` are especially dangerous in regard to security. We recommend you deactivate these services in the `inetd.conffile` unless you need them for specific purposes.

- **Services such as Network Information System (NIS) or Network File System (NFS)**

  You can use the Network Information System (NIS) to manage user data and passwords centrally. This service allows every UNIX machine in a local area network to read the password file using the `ypcat passwd` command, including shadow password files.

  Another service is the Network File System (NFS) service. This service makes directories available across the network. It is a service that is also frequently used in the SAP System environment to make transport and work directories accessible over the network.

  There are certain security risks involved when using these services and you should take special precautions. For example, when using NFS, you should be cautious when determining which directories should be made available. Do not export directories that contain SAP data to arbitrary recipients using NFS. Export to known and "trustworthy" systems only. Be cautious when assigning write authorization for NFS paths and avoid distributing the home directories of users across NFS.

- **X Windows**

  There are security issues involved with the use of X Windows. Therefore, for an SAP Web AS installation, you should check and see if you need to have the corresponding X server running on an SAP application server. If not, then disable this service. Otherwise, take precautions according to your vendor to protect this service.

- **Summary**

  To summarize the precautions that you should take, especially pertaining to NIS, NFS and the BSD remote services, adhere to the following guidelines:

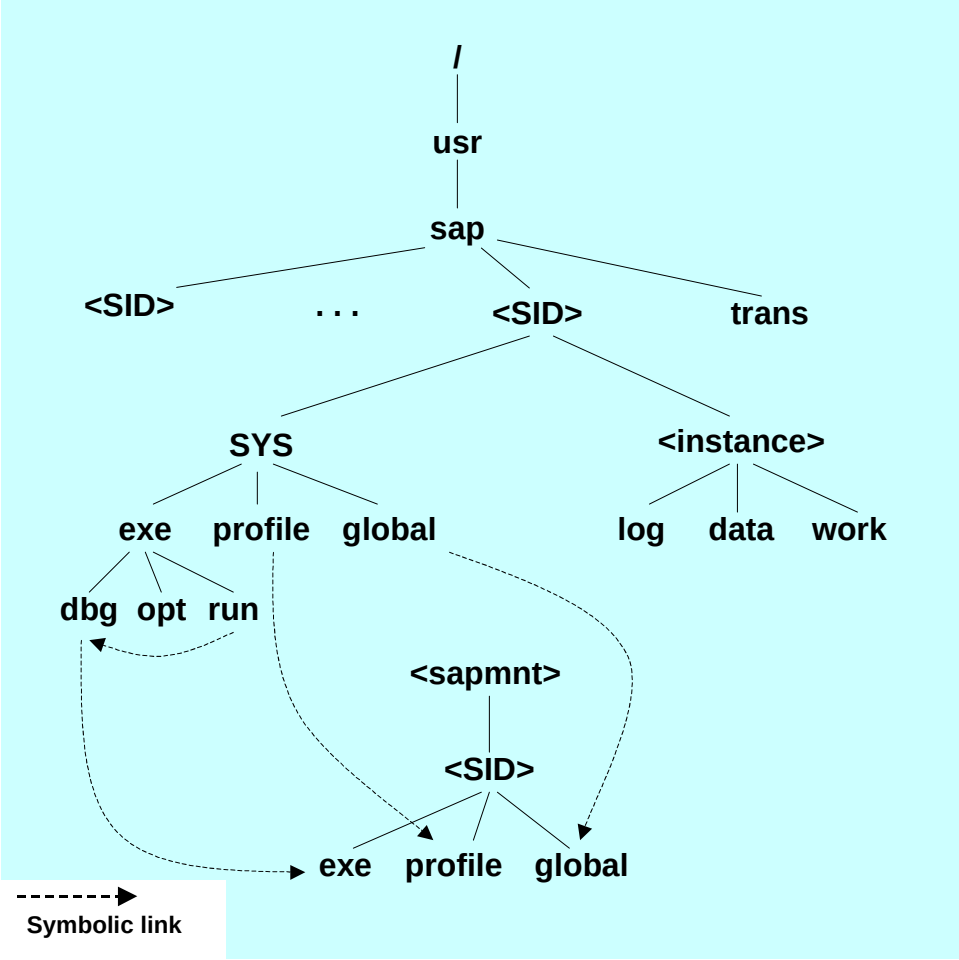
  - Disable any services that you do not need.
  - To ensure a safe environment when using any of these services, follow the instructions of your OS vendor. Also use tools for monitoring activities to help you detect potential misuse of these services.
  - If you do use these services, then use them only within a secure LAN.
  - Do not export directories that contain SAP data to arbitrary recipients using NFS. Export to "trustworthy" systems only.
  - Protect the following users: `root`, `<sid>adm` and `<db><sid>`. These should be the only users that exist on your application servers and your main instance at the operating system level. After installation, you should lock `<db><sid>` on your application servers.
  - For critical users, empty the `.rhosts` files and assign it the access rights "`000`".
  - Either delete the file `/etc/hosts.equiv` or make sure that it is empty.
  - Keep your operating system up to date regarding security-related patches that are released by your operating system vendor!

3 Protected SAP System Directory Structures Under UNIX/LINUX

For security reasons, the SAP System together with the user data is stored in a special directory structure in the operating system and is protected with defined access authorizations.

The graphic below shows how the SAP System directory structure is established in the UNIX/LINUX file system:

SAP System Directory Structure Under UNIX/LINUX



4 Setting Access Privileges for SAP System Directories Under UNIX/LINUX

We recommend that you restrict the file and directory access privileges as shown in the table below.

The access rights shown in the table below are automatically set in the installation procedures.

Setting Access Privileges for SAP System Directories and Files

SAP Directory or Files	Access Privilege in Octal Form	Owner	Group
/sapmnt/<SID>/exe	775	<sid>adm	sapsys
/sapmnt/<SID>/exe/saposcol	4755	root	sapsys
/sapmnt/<SID>/global	700	<sid>adm	sapsys
/sapmnt/<SID>/profile	755		
/usr/sap/<SID>	751		
/usr/sap/<SID>/<Instance ID>	755		
/usr/sap/<SID>/<Instance ID>/*	750	<sid>adm	sapsys
/usr/sap/<SID>/<Instance ID>/sec	700	<sid>adm	sapsys
/usr/sap/<SID>/SYS	755	<sid>adm	sapsys
/usr/sap/<SID>/SYS/*	755	<sid>adm	sapsys
/usr/sap/trans	775	<sid>adm	sapsys
/usr/sap/trans/*	770	<sid>adm	sapsys
/usr/sap/trans/.sapconf	775	<sid>adm	sapsys
<home directory of <sid>adm>	700	<sid>adm	sapsys
<home directory of <sid>adm>/*	700	<sid>adm	sapsys

UMASK

Newly created files have rights determined by UMASK definitions. An UMASK is a four digit octal number that specifies those access rights that are **not** to be given to newly created files. You can define UMASKS in any of several files, to include:

- `.login`
- `.cshrc`
- `.profile`
- `/etc/profile`

As with UNIX access rights, the corresponding octal positions represent user, group, and world access, and the value of the digit represents which access privileges should be removed (remove none = 0, remove write = 2, remove all = 7).

You can use the UMASK to automatically restrict permissions for newly created files. For example, by defining a UMASK of 0027, you specify that all newly created files have the access rights 750.

5 Setting Rights for an Installation with Several SAP Systems

If there are several SAP systems on the server(s), it is possible to perform the administration tasks separately using different groups. Assign the access rights appropriately for the files in the directory `\usr\sap` (to include sub-directories). You can distinguish between the administrators and groups by using the system IDs of the SAP systems (for example, `sapsys<SAPSID1>`, and `sapsys<SAPSID2>`). All administrators should have access to the two directories at the `\usr\sap` top level.

If there are several SAP systems installed on a single server, then an additional area of shared memory exists. This memory is created by `saposcol` and is used jointly by the OS Collector and all SAP systems. Therefore, give full control access rights to the `sapsys<SAPSIDx>` groups for the executable file `saposcol`. To avoid access conflicts here, start `saposcol` before starting the first SAP system.

6 Additional Information on UNIX/LINUX Security

Type	Title
Internet	Cipher: Electronic Newsletter of the Technical Committee on Security and Privacy: http://www.ieee-security.org/cipher.html Computer Emergency Response Team (CERT): http://www.cert.org Linux security: http://www.linuxsecurity.com/