ผู้ใช้ขั้นสูง

ในการคำนวณ**superuser**คือบัญชีผู้ใช้พิเศษที่ใช้สำหรับการดูแลระบบ ทั้งนี้ขึ้นอยู่กับระบบปฏิบัติการ (OS) ชื่อจริงของบัญชีนี้อาจจะมี**ราก** , **ผู้ดูแล** , **ผู้ดูแลระบบ**หรือผู้บังคับบัญชา ในบางกรณี ชื่อจริงของบัญชีไม่ใช่ปัจจัยกำหนด ในระบบที่คล้าย Unix ตัวอย่างเช่น ผู้ใช้ที่มีตัวระบุผู้ใช้ (UID) เป็นศูนย์คือ superuser โดยไม่คำนึงถึงชื่อของบัญชีนั้น [1]และในระบบที่ใช้โมเดลความปลอดภัยตามบทบาท ผู้ใช้ที่มีบทบาท superuser (หรือคำพ้องความหมาย) สามารถดำเนินการทั้งหมดของบัญชีผู้ใช้ superuser ได้ หลักการของสิทธิน้อย ขอแนะนำให้ผู้ใช้และแอปพลิเคชันส่วนใหญ่ทำงานภายใต้บัญชีปกติเพื่อทำงาน เนื่องจากบัญชีผู้ใช้ขั้นสูงสามารถทำการเปลี่ยนแปลงทั่วทั้งระบบได้โดยไม่มีข้อจำกัด อาจเป็นผลเสีย

Unix และ Unix เหมือน

In Unix-like computer OSes (such as Linux), *root* is the conventional name of the user who has all rights or permissions (to all files and programs) in all modes (single- or multi-user). Alternative names include *baron* in BeOS and *avatar* on some Unix variants.[2] BSD often provides a *toor* ("root" written backward) account in addition to a root account.[3] Regardless of the name, the superuser always has a user ID of 0. The root user can do many things an ordinary user cannot, such as changing the ownership of files and binding to network ports numbered below 1024.

The name *root* may have originated because *root* is the only user account with permission to modify the root directory of a Unix system. This directory was originally considered to be root's home directory,[4] but the UNIX Filesystem Hierarchy Standard now recommends that root's home be at `/root`.[5] The first process bootstrapped in a Unix-like system, usually called `init`, runs with root privileges. It spawns all other processes directly or indirectly, which inherit their parents' privileges. Only a process running as root is allowed to change its user ID to that of another user; once it has done so, there is no way back. Doing so is sometimes called *dropping root privileges* and is often done as a security measure to limit the damage from possible contamination of the process. Another case is `login` and other programs that ask users for credentials and in case of successful authentication allow them to run programs with privileges of their accounts.

It is often recommended that *root* is never used as a normal user account,[6][7] since simple typographical errors in entering commands can cause major damage to the system. Instead, a normal user account should be used, and then either the `su` (substitute user) or `sudo` (substitute user do) command is used. The `su` approach requires the user to know the root password, while the `sudo` method requires that the user be set up with the power to run "as root" within the `/etc/sudoers` file, typically indirectly by being made a member of the *wheel*,[8] *adm*,[9] *admin*, or *sudo* group.

For a number of reasons, the `sudo` approach is now generally preferred – for example it leaves an audit trail of who has used the command and what administrative operations they performed.[10]

Some OSes, such as macOS and some Linux distributions (most notably Ubuntu[6]), automatically give the initial user created the ability to run as root via `sudo` – but configure this to ask them for their password before doing administrative actions. In some cases the actual *root* account is disabled by default, so it can't be directly used.[6] In mobile platform-oriented OSs such as Apple iOS and Android, superuser access is inaccessible by design, but generally the security system can be exploited in order to obtain it. In a few systems, such as Plan 9, there is no superuser at all.[11]

Microsoft Windows

In Windows NT and later systems derived from it (such as Windows 2000, Windows XP, Windows Server 2003, and Windows Vista/7/8/10), there must be at least one administrator account (Windows XP and earlier) or one able to elevate privileges to superuser (Windows Vista/7/8/10 via User Account Control).[12] In Windows XP and earlier systems, there is a built-in administrator account that remains hidden when a user administrator-equivalent account exists.[13] This built-in administrator account is created with a blank password.[13] This poses security risks as local users would be able to access the computer via the built-in administrator account if the password is left blank, so the account is disabled by default in Windows Vista and later systems due to the introduction of User Account Control (UAC).[13] Remote users are unable to access the built-in administrator account.

A Windows administrator account is not an exact analogue of the Unix root account – Administrator, the built-in administrator account, and a user administrator account have the same level of privileges. The default user account created in Windows systems is an administrator account. Unlike macOS, Linux, and Windows Vista/7/8/10 administrator accounts, administrator accounts in Windows systems without UAC do not insulate the system from most of the pitfalls of full root access. One of these pitfalls includes decreased resilience to malware infections. To avoid this and maintain optimal system security on pre-UAC Windows systems, it is recommended to simply authenticate when necessary from a standard user account, either via a password set to the built-in administrator account, or another administrator account.

In Windows Vista/7/8/10 administrator accounts, a prompt will appear to authenticate running a process with elevated privileges. Usually, no user credentials are required to authenticate the UAC prompt in administrator accounts but authenticating the UAC prompt requires entering the username and password of an administrator in standard user accounts. In Windows XP (and earlier systems) administrator accounts, authentication is not required to run a process with elevated privileges and this poses another security risk that led to the development of UAC. Users can set a process to run with elevated privileges from standard accounts by setting the process to "run as administrator" or using the `runas` command and authenticating the prompt with credentials (username and password) of an administrator account. Much of the benefit of authenticating from a standard account is negated if the administrator account's credentials being used has a blank password (as in the built-in administrator account in Windows XP and earlier systems), hence why it is recommended to set a password for the built-in administrator account.

In Windows NT, 2000 and higher, the root user is the Administrator account.[14]

โนเวลล์ เน็ตแวร์

In Novell NetWare, the superuser was called "supervisor",[15] later "admin".

OpenVMS

In OpenVMS, "SYSTEM" is the superuser account for the OS.

ระบบส่วนบุคคลที่เก่ากว่า

On many older OSes on computers intended for personal and home use, anyone using the system had full privileges. Many such systems, such as DOS, did not have the concept of multiple accounts, and although others such as Windows 95 did allow multiple accounts, this was only so that each could have its own preferences profile – all users still had full administrative control over the machine.

ดูสิ่งนี้ด้วย

- nobody (username)
- passwd
- Power user
- Rooting (Android OS)
- Rootkit
- Privilege escalation
- sudo
- Jailbreaking (iOS)

อ้างอิง

1. *"getpwuid" (http://pubs.opengroup.org/onlinepubs/009695399/functions/getpwuid.html) . opengroup.org. Retrieved 12 January 2019.*
2. *The Jargon File (version 4.4.7) (http://www.catb.org/jargon/html/A/avatar.html) , catb.org*
3. *"What is this UID 0 toor account?" (http://www.freebsd.org/doc/en_US.ISO8859-1/books/faq/security.html#TOOR-ACCOUNT) , freebsd.org*
4. *"What is root? - definition by The Linux Information Project" (http://www.linfo.org/root.html) . LINFO. Retrieved 2012-08-07.*
5. *"/root : Home directory for the root user (optional)" (http://www.pathname.com/fhs/pub/fhs-2.3.html#ROOTHOMEDIRECTORYFORTHEROOTUSER) .*
6. *"RootSudo" (https://help.ubuntu.com/community/RootSudo) . ubuntu.com. Retrieved 16 September 2015.*
7. *"4.4. Administrative Controls" (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s1-wstation-privileges.html) . redhat.com. Retrieved 16 September 2015.*
8. *"2.3. Configuring sudo Access" (https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux_OpenStack_Platform/2/html/Getting_Started_Guide/ch02s03.html) . redhat.com. Retrieved 16 September 2015.*

9. *"difference adm - root" (http://www.linuxquestions.org/questions/linux-newbie-8/difference-adm-root-536387/) . Retrieved 1 August 2016.*
10. *Brian Wotring (2005). Host Integrity Monitoring Using Osiris and Samhain (https://books.google.com/books?id=CGE2synNNSEC&pg=PA32) . Elsevier. p. 32. ISBN 978-0-08-048894-3.*
11. *"Security in Plan 9" (http://plan9.bell-labs.com/sys/doc/auth.html) , Bell Labs*
12. *"Microsoft Corporation" (https://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/ua_c_account_types.mspx?mfr=true) . Microsoft.com. Retrieved 2012-08-07.*
13. *"Enable and Disable the Built-in Administrator Account" (https://technet.microsoft.com/en-us/library/cc766343(WS.10).aspx) . microsoft.com. Retrieved 2014-02-26.*
14. *"The LocalSystem Account" (http://msdn.microsoft.com/en-us/library/ms677973%28v=vs.85%29.aspx) . microsoft.com. Microsoft. Retrieved 16 September 2015.*
15. *"Supervisor (Bindery) User Created on Every NetWare 4 Server" (https://support.novell.com/techcenter/tips/ant19960203.html) , 01 Feb 1996, novell.com*

ลิงค์ภายนอก

Look up ***superuser*** in Wiktionary, the free dictionary.

- root Definition (http://www.linfo.org/root.html) - by The Linux Information Project (LINFO)
- An Introduction to Mac OS X Security (https://web.archive.org/web/20040305061552/http://developer.apple.com/internet/security/securityintro.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Superuser&oldid=1055646792"

แก้ไขล่าสุดเมื่อ15 วันก่อนโดยLizardJr8