

Úloha správce OS a správce sítě

Úlohou správného správce systému a sítě je pouze mít nohy na stole a sledovat, jak je vše správně nastaveno a zkonfigurováno a sledovat pouze provoz - ideální stav.

Povinnosti *správce systému* je neustále sledovat chování operačního systému.

Správce sít :

- nastavení routování, ip adresace
- nastavení firewall
- rozčleňuje logickou strukturu sítě

Základem bezpečnosti systému je dobrá systémová administrace. Ta zahrnuje kontrolu vlastnictví a přístupových práv ke všem životně důležitým souborům a adresářů, a sledování používání privilegovaných účtů.

Při zpřístupňování určité služby přes síť jí vždy přidejte nejnižší práva, což znamená, že jí nedovolíte provádět věci, které pro své fungování nepotřebuje.

Dále je nutné se vyhnout "nebezpečným" aplikacím. Programy, které vyžadují speciální přístupová práva, jsou logicky nebezpečnější než jiné.

Instalace, správa a údržba systému

Nutná volba souborového systému. Klasický (FAT32, NTFS, Ext2) potřebuje po náhlém výpadku energie provést kontrolu konzistence disku (scandisk, fsck, chdsk).

Journaling - založen na databázovém systému (princip relací, a el bez podpory rollback).

Při výpadku energie je k dispozici přehled o probíhajících operacích - ext3, ReiserFS, XFS, pomalejší zápis na disk

LVM (Logical Volume Manager) - logický manažer svazků

Díky LVM je vytvořena dodatečná vrstva mezi fyzickou periferií a I/O rozhraním v jádře. LVM v zásadě umožňuje zřetězovat jednotlivé disky z diskového pole a pohlíží na ně jako na nová logická zařízení. Je možné za běhu přidat další disky a zvětšit jednotlivé svazky o jejich prostor.

Správa a údržba systému

Nutné aktualizace systému. U systému Windows je důležitá antivirová ochrana systému.

Volba vhodného antivirového programu a včasná aktualizace virové databáze.

Pravidelné dávkové operace - údržba, kontrola práv,...

Správa uživatelských účtů a monitorování činnosti uživatelů

Uživatel: adduser nemo, passwd nemo, deluser -r nemo (parametr r - odebrání home)

Skupina

Každý uživatel systému musí náležet alespoň do jedné uživatelské skupiny. Může ale také patřit do více skupin. Tímto způsobem je možné snadno kombinovat práva tak, aby byla na míru ušita konkrétnímu uživateli a jeho potřebám. addgroup+ groupdel

Práva souborů

r - čtení souboru (zobrazení, zkopírování, tisk,..)

w - zápis do souboru

Správa operačních systémů

x - spuštění souboru jako programu

Práva adresářů

r - vypsat jména souborů a podadresářů

w - spolu s právem x umožňuje vytvářet, rušit a přejmenovávat soubory a podadresáře

x - vypsat informace o souboru nebo podadresáři se známým jménem, je podmínkou pro všechny operace s obsahem adresáře kromě vypsaní jmen

chmod slouží ke změně práv souboru, umask zobrazuje nebo nastavuje implicitní masku práv pro nově vytvářené soubory

Rozšířená práva

s pro uživatele *setuid*, s pro skupinu *setgid*, t pro ostatní *sticky*

Program s nastaveným *setuid* bitem disponuje při běhu právy svého vlastníka. (uživatel si mění heslo, zápis má právo root. Podobně funguje *setgid* - skupina mail. *Sticky* bit u adresáře vyjadřuje, že do adresáře má právo zapisovat a číst každý, avšak mazat může pouze vlastník adresáře.

Monitorování uživatelů

Politika hesel

správně zvolené heslo by mělo odpovídat kritériím:

- nemělo by mít souvislost s vaší osobou
- nemělo by se jednat o existující slovo
- měli byste používat kombinaci velkých/malých písmen, číslic a alfanumerických znaků

co nedělat:

- poznamenávat si heslo v jakékoli nezašifrované podobě
- používat jedno heslo pro všechny účely

Úkoly správce:

- nastavit minimální délku hesla
- nastavit časově omezení doby platnosti hesla
- omezit počet neúspěšných pokusů o přihlášení
- školit uživatele
- přidělovat pouze individuální hesla

Správa a údržba souborových systémů, archivace, zálohování

Archivace - dlouhodobé uložení dat, zpravidla spojená s kompresí (gzip, zip, rar)

Zálohování - tvorba krátkodobějších záloh - inkrementální záloha, celá záloha

Pro zálohu celého systému volíme programy dd nebo typu ghost.

RAID - Redundant Array of Independent Disks, lze provozovat HW, SW, HW/SW

Existuje šest typů polí, ale prakticky se používají RAID 0,1,5

Správa operačních systémů

RAID 0 (Nonredundant striped array)

- Základní jednotkou pole je tzv. stripe
- Po sobě jdoucí data jsou pak v poli rozložena střídavě mezi disky do stripů tak, aby se při sekvenčním čtení/zápisu přistupovalo ke všem diskům současně -> maximální rychlost
- S rostoucím počtem disků v poli roste i pravděpodobnost výpadku pole
- RAID 0 je velmi rychlý, ale méně bezpečný než samostatný disk

RAID 1 (Mirrored array)

- maximálně redundantní
- rychlost čtení může být oproti samostatnému disku výrazně vyšší, rychlost zápisu je stejná jako u samostatného disku
- data jsou při zápisu zrcadlena na všechny disky v poli
- čím více disků, tím větší redundance a odolnost proti výpadku

RAID 5 (Striped array with rotating parity)

- redundance vůči výpadku libovolného jednoho disku
- parita není uložena na jednom vyhrazeném disku, ale je rozmístěna rovnoměrně mezi všemi disky pole

Správa síťových služeb

cokoli, co pracuje se sítí/porty, je síťová služba

echo 7, ssh 22, ftp 21,22, telnet 23, smtp 25, nameserver 42, imap 143, https 443, www 80, finger 79, samba 137, 138, 139

spuštěny pouze nezbytné služby s nezbytnými právy

Pokud služba očekává delší provoz na portu, přepne se na jiný port, aby well known byl volný.

NTP server - synchronizace času

FTP

DHCP

dynamické přidělování adres z předem zadaného rozsahu lze nastavit podle mac adresy, že určité zařízení bude mít stále stejnou adresu. DHCP nikdy nepřiděluje adresy routerům, switchům a serverům tyto zařízení potřebují statické adresy. Adresy se přidělují na určitý čas a pak musí klientský počítač znovu žádat o přidělení adresy. Tato adresa nemusí být stejná, ale typicky pokud není obsazena, je mu přidělena stejná adresa.

DNS

služba zajišťující překlad IP adres na jejich jmenné ekvivalenty a nazpět jménem určené adresy na jejich IP adresu. Na jednom PC v síti je nainstalována služba DNS. Pokud záznam v tabulce neexistuje, zeptá se systém dalších DNS serverů, jejichž adresy má definované, případně vrátí chybovou odezvu.

Web server

umožňuje uživatelům přístup k webovým stránkám, které jsou na tomto serveru umístěny.

Samba

SMB protokol, identický protokolu CIFS (od MS); SMB je obdoba NFS ve win prostředí