Projekt v rámci SIPVZ:

IMPLEMENTACE OPERAČNÍHO SYSTÉMU LINUX DO VÝUKY INFORMAČNÍCH TECHNOLOGIÍ

LINUX

Lekce 21

Základní administrace - 3

Obsah lekce:

Cíle

Po skončení této lekce studenti budou schopni:

- Připojit disketu nebo CD-ROM mechaniku a vyjmenovat komponenty potřebné pro Popsat komponenty Linuxu pro tisk a konfiguraci tiskárny.
- Mít přehled a monitorovat systém

Připojování disket a CD-ROMů

- Připojování a odpojování disket
  - Musí být zadán přípojný bod
  - Pokud nebude dále používat pak odpojte
- Připojování a odpojování CD-ROM
  - mount –t iso9660 /dev/cdrom /mnt/cdrom
- Připojení cizího souborového systému
  - mount –t vfat (dev/hda7/ /mnt/windows_d
- Možnosti automatického připojení

Pro připojení cizích přístupových médií (disket, cd-romů) vždy používejte příkaz mount. Základní syntaxe příkaz mount je následující:

```
mount [-fnrsvw] [-t vfstype] [-o options] device dir
```

Přepínač –t je používán ke specifikování typu souborového systému, který má být připojen. Device je fyzické zařízení, které má být připojeno. Dir je bod jako který bude zařízení připojeno.

Připojování a odpojování disket

Jestliže si uživatel přeje připojit disketu, která byla naformátována pro Linux, stačí použít něco jako toto:

```
$ mount /dev/fd0 /floppy
```

Tento příkaz připojí /dev/fd0/ jako přípojný bod /floppy. Na rozdíl od Windows Linux zachází se všemi připojenými zařízeními a jejich souborovým systémem jakoby byly součástí lokálního souborového systému, proto musí být specifikován přípojný bod. Přístup k datům na disketě pod Linuxem je výborný zadáním přípojného bodu jako by to byl nějaký jiný adresář.

```
$ cd /floppy
```

Pro odpojení disket by měl být použit příkaz umount ve stejném tvaru jako byl použit příkaz mount:

```
$ umount /dev/fd0 /floppy
```

Disketa nebo jakékoliv jiná vyměnitelná média by měla vždy být odpojena, pokud nebudou dále používána. Jednoduché vysunutí média není dostatečné, protože toto neodstraní připojený bod zobrazený v souborovém systému.

Připojování a odpojování CD-ROMu

Připojení CD-ROMu probíhá stejnou cestou jako připojení diskety. Po vložení CD-ROMu do mechaniky, může být disk připojen následujícím příkazem:

```
$ mount /dev/cdrom /cdrom
```

Tento příklad připojí CD v CD-ROM mechanice /dev/cdrom jako přípojný bod /cdrom. Pro odpojení CD-ROMu se opět použije příkaz umount stejným způsobem jako u diskety.

```
$ umount /dev/cdrom /cdrom
```

Připojení cizího souborového systému

Pro připojení souborového systému použijte přepínač –t v příkazu mount. Například disk formátovaný pomocí FAT32 nebo VFAT souborovým systémem může být připojen následovně:

```
$ mount –t vfat /dev/fd0 /98floppy
```

Přepínač –t je použit k určení typu souborového systému, který má být připojen. Přípojný bod byl zvolen, tak aby odpovídal jeho typu. Jestliže je souborový systém určen v souboru /etc/vstav pak nemusí být specifikován v příkazové řádce. Pro kompletní seznam odlišných souborových systému, které mohou být připojeny, zkontrolujte man stránky pro mount.

Jiná velká volba se naskýtá uživatelům se strojem s dvěma operačními systémy, neboť mohou připojit FAT nebo FAT32 oblast do jejich adresářového stromu. Toto učiní data na této oblasti uložená ve Windows stejně dobře v Linuxu.

Pro příklad disková oblast na stejném stroji formátovaná pomocí FAT32 nebo VFAT souborovým systémem může být připojena následujícím:

```
$ mount –t vfat /dev/hda7 /mnt/windows_d
```

Automatické připojování – automount

Automount dovoluje automatické připojování a odpojování zařízení nebo souborových systémů pomocí démona. V případě že se uživatel pokouší přistupovat na nepřipojené zařízení, démon ho připojí automaticky. Hlavní dva Linuxové nástroje pro automount jsou AMD a autofs. Zatímco AMD nepožaduje podporu kornelu, novější autofs ano. Možná budete muset překompilovat Váš kornel k odblokování autofs. Více informací o AMD a autofs naleznete na

http://www.linuxdoc.org/HOWTO/mini/Automount.html.

Monitoring systému

- Evidence procesů
  - **ps, who, w, top**
  - Vlastníci procesů
  - Vytížení CPU a paměti
  - Priorita a umístění procesů
- Správa úložného prostoru
  - **df** – zobrazí volné místo na disku (s –h)
  - **du** – zobrazuje využití místa uživatelem
- Monitoring sítě
  - **netstat** a **nmap** – informace o stávajících službách a portech

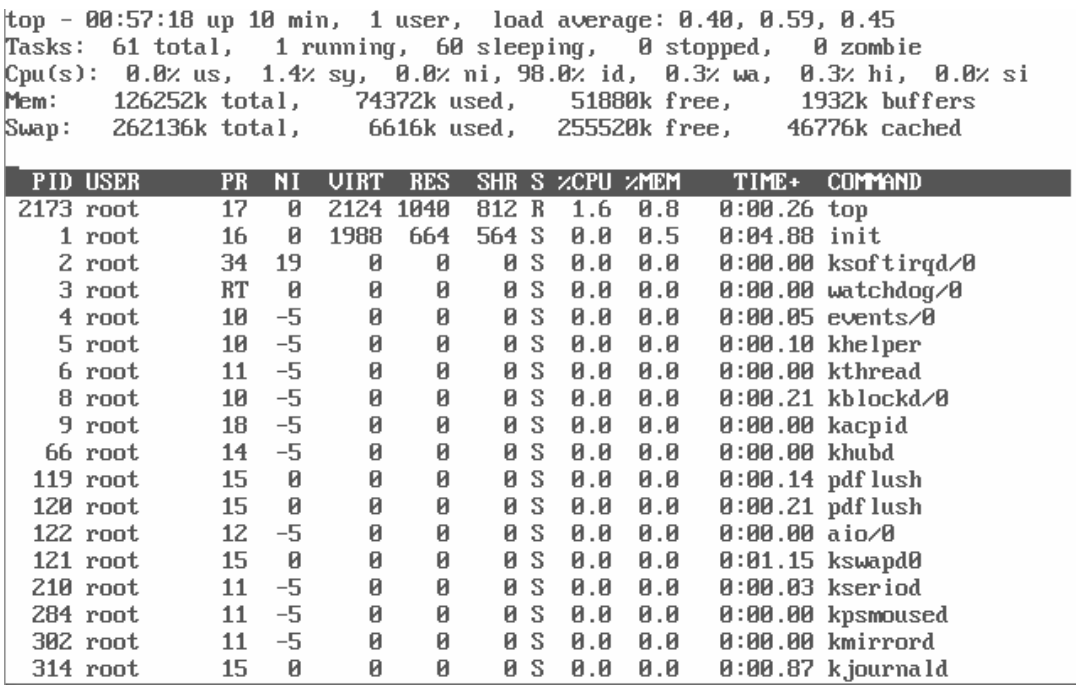
V této části je probráno několik základních měření, které mohou být použity pro sledování stavu (zdraví) systému. Je zde mnoho rozličných příčin proč si administrátor přeje sledovat stav systému, nejvíce důležitou je bezpečnost. Administrátor často monitoruje procesy běžící v systému, aby zkontroloval možnost proniknutí nějakého nebezpečí. Ačkoliv je bezpečnost zásadní důvod pro monitoring systému, administrátor obyčejně monitoruje systém, aby zajistil, že všichni uživatelé mohou spravedlivě využívat a sdílet zdroje systému. Z tohoto důvodu se sledují zdroje jako procesy, úložná zařízení a síť. Tudíž může být monitoring systému shrnut do základních tří kategorií:

- Evidence procesů
- Správa úložního procesu
- Monitoring sitě

Evidence procesů

Tato část pokrývá základní techniky a příkazy, které mohou vykonávat monitoring procesů.

Některé základní příkazy, které mohou být použity jsou: ps, who, w a top. Použitím těchto příkazů administrátor může dostat výpis obrazovky procesů, které aktuálně běží v systému, vlastníky procesů, čas CPU, velikost paměti využité procesy, jejich prioritu a umístění odkud byly spuštěny. Obdržením tolika detailů může administrátor přesně vymezit uživatelům užití systémového času a regulovat využití procesoru a paměti redukováním priority jednotlivých procesů. Následuje ukázka výstupu příkazu top:



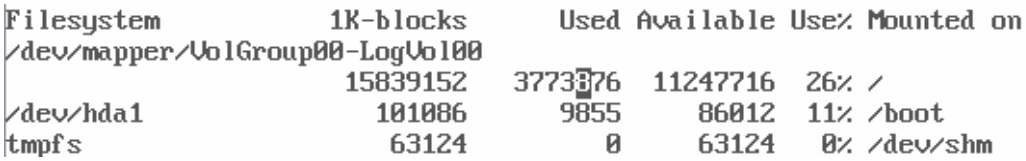
Obrázek 21-1 – Výstup příkazu top

Předchozí příkaz je také zásadní pro bezpečnostní účely. Proces, který si přivlastňuje CPU nebo paměť, který byl spuštěn z nedůvěryhodného zdroje by mohl mýt záškodnické úmysly. Použitím těchto příkazů můžete dosáhnout základního monitoringu procesů a tím předejít riziku.

Správa úložného prostoru

Ze stejného důvodu je také správa úložného prostoru velmi podstatná. Problémy s úložištěm mohou představovat bezprostřední hrozbu jako nedostatek místa pro soubory uživatelů a pokles výkonnosti. Nástroje jako df a du poskytují informace o jednotlivých uživatelských discích a souborových systémech.

Častou příčinou nedostatku místa na souborovém systému bývají log soubory a maily. Dohlédněte na uložení logů a mailů do odlišných oblastí. Jedna z hlavních příčin pro dosažení diskové kvóty uživatele bývají vytvořené soubory vytvořené po spadnutí programu. Neustále udržujte na paměti nebo využitím nějakého automatického nástroje či skriptu řešení těchto problémů. Následuje výpis příkazu df:



Obrázek 21-2 – Výstup příkazu df

Poznámka: Když používáte příkaz df je velmi užitečné připojit přepínač –h (human output), ten zobrazí velikost v megabytech místo v diskových blocích. Zkušenější matematici a fyzici mohou bezpečně tuto možnost ignorovat.

Následující příklad výpisu příkazu du –s . in kilobytes:

```
$ du –s
546108
```

Monitoring sítě

Rozmanité nástroje monitoringu sítě jsou dostupné pro detekci pronikání do systému a mezer v bezpečnosti. Nástroje jako netstat a nmap podávají detailní informace týkající se služeb a portů, které jsou v systému aktivní. Tyto nástroje mohou být využity pro sestřelení jakékoliv nedostatečně chráněné služby.

Pro monitorování spojení - netsat

Příkaz netstat je užitečný mnoha způsoby, tři jsou specifické.

Zobrazení směrové tabulky (route table):

```
# netstat –nr
```

```
Směrovací tabulka v jádru pro IP
Adresát         Brána           Maska           Přízn   MSS Okno    irtt Rozhran
í
192.168.1.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
0.0.0.0         192.168.1.1     0.0.0.0         UG        0 0          0 eth0
```

Zobrazením statistiky pro rozhraní:

```
[user@host]$ netstat –i
```

Tabulka rozhraní kernelu:

```
Tabulka rozhraní v jádru
Iface       MTU Met    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR
Flg
eth0       1500   0       22      0      0      0       23      0      0      0
BMRU
lo        16436   0      433      0      0      0      433      0      0      0
LRU
```

Zobrazením spojení z a do počítače:

```
[root@localhost ~]# netstat -ta
Aktivní Internetová spojení (servery a navázaná spojení)
Proto Recv-Q Send-Q Local Address               Foreign Address             Stat
e
tcp        0      0 *:sunrpc                    *:*                         LIST
EN
tcp        0      0 localhost.localdomain:50000 *:*                         LIST
EN
tcp        0      0 localhost.localdomain:50002 *:*                         LIST
EN
tcp        0      0 localhost.localdomain:ipp   *:*                         LIST
EN
tcp        0      0 *:43319                     *:*                         LIST
EN
tcp        0      0 localhost.localdomain:smtp  *:*                         LIST
EN
```

Nmap je skvělá utilita třetí strany, která funguje s každou distribucí. Je to užitečný nástroj pro skenování portů ve velkých sítích, kde všechny cesty vedou do samostatných počítačů.

Nmap má rozhraní příkazové řádky, i když je dostupný i s grafickým vzhledem, dělá život trochu snadnější pro velmi vytížené administrátory.

Nmap a jeho grafický vzhled najdete na http://www.insecure.org/nmap/index.html.