Hálózati operációs rendszerek
NGB_TA047_1
6. kisZH
2011. 10. 24.

Ahol másként nem jeleztük, minden feladat helyes megoldása 1 pontot ér. Értékelés: 6 ponttól elégséges, 7-től közepes, 8-tól jó, 9-től jeles.

1. Írjon olyan **iptables** szabályt, amely a géphez SSH-val való csatlakozásokat "**SSH: **" prefix-szel naplózza!
   ```
   iptables -A INPUT -p tcp --dport 22 --syn \
   -j LOG --log-prefix "SSH: "
   ```
2. Sorolja fel a rendszernaplózásnál használt prioritási szinteket szabványos megnevezéssel, sorrendben a legfontosabbtól a legkevésbé fontosig! (Ügyeljen a helyes megnevezésekre!)
   emerg, **alert**, **crit**, **err**, **warning**, **notice**, **info**, **debug**
3. Mely könyvtárban levő, milyen nevű fájlban kell megadni a **sysklogd** beállításait?
   /etc/syslog.conf
4. Mit ír a **sysklogd** konfigurációs állományába ahhoz, hogy a **root** felhasználó minden autentikációs eseményről azonnal értesítést kapjon?
   ```
   auth.*    root
   ```
5. Mit ír a **sysklogd** konfigurációs állományába ahhoz, hogy minden nyomtatással kapcsolatos, hiba szintű vagy annál súlyosabb esemény naplóüzenete (naplózás céljából) a **log.cegem.hu** gépre elküldésre kerüljön?
   ```
   lpr.err   @log.cegem.hu
   ```
6. Mit eredményez a **sysklogd** konfigurációs állományában a következő bejegyzés?
   ```
   *.=notice;lpr.none  -/var/log/notices.log
   ```
   A nyomtatással kapcsolatos üzenetek kivételével az összes pontosan **notice** szintű naplóüzenet a /var/log/notices.log nevű fájlba naplózódik, gyorsítótárazással.
7. Miből derül ki, hogy amit a **sysklogd** konfigurációs állományában az action mezőben megadtunk, az terminál, névvel ellátott csővezeték (name pipe), fájl, távoli gép vagy felhasználó neve-e?
   terminál: az action mezőben **/dev/<terminál neve>** van megadva
   névvel ellátott csővezeték: az action a pipe ("**|**") jellel kezdődik
   fájl: egy teljes útvonallal megadott fájlnév van megadva (nem pontos, de azt is elfogadjuk, hogy: az action a "**/**" karakterrel kezdődik és utána nem terminál áll)
   távoli gép: az action a "**@**" karakterrel kezdődik
   felhasználó: az action "**[^|/@]**" karakterrel kezdődik (magyarázat: a kezdő karakter NEM a "**|**", "**/**", "**@**" karakterek közül való)
8. Mely könyvtárban levő, milyen nevű fájlban kell megadni a **syslog-ng** beállításait?
   /etc/syslog-ng/syslog-ng.conf
9. Adja meg az alábbi **sysklogd** konfigurációs bejegyzéseknek megfelelő **syslog-ng** beállításokat! Használja az **s_all** forrásdefiníciót, és adjon meg minden mást! (2x1 pont)
   ```
   kern.*    /var/log/kern.log
   destination df_kern { file("/var/log/kern.log"); };
   filter f_kern { facility(kern); };
   log {
        source(s_all);
        filter(f_kern);
        destination(df_kern);
   };
   ```

```
cron.err  |/dev/xconsole
destination dp_xconsole { pipe("/dev/xconsole"); };
filter f_cron { facility(cron); };
filter f_at_least_err { level(err..emerg); };
log {
     source(s_all);
     filter(f_cron);
     filter(f_at_least_err);
     destination(dp_xconsole);
};
```