

LINUX RENDSZERFEJLESZTÉS ÉS ÜZEMELTETÉS

4. forduló



A kategória támogatója: One Identity - Quest
Hungary

Ismertető a feladatlaphoz

Közeleg az 5. forduló, figyelj az időpontokra!

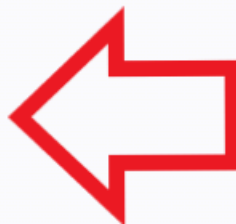
Használd a naptárat:

KATEGÓRIÁIM

Összesen 10 kategóriára jelentkezted



Versenynaptár letöltése



Vagy figyeld kategóriánként az időpontokat (íme egy MINTA, hol találod):

● 3. FORDULÓ




A lezárt fordulókban eddig megszerzett pontok:

0/100 pont

**BOSCH**

Invented for life

Fordulók

Forduló	Pontok, időtartam		Feladat megoldható	Státusz
7. forduló	23 pont 25:00		2023.11.28. 20:00-tól 2023.11.28. 20:35-ig	Feladatlap
6. forduló	23 pont 30:00		2023.11.21. 20:00-tól 2023.11.21. 20:40-ig	Feladatlap
5. forduló	28 pont 25:00		2023.11.14. 20:00-tól 2023.11.14. 20:35-ig	Feladatlap

Amennyiben olyan kategóriában játszol, ahol van csatolmány, de hibába ütközel a letöltésnél, ott valószínűleg a vírusirtó korlátoz, annak ideiglenes kikapcsolása megoldhatja a problémát. (Körülbelül minden 3000. letöltésnél fordul ez elő.)

Jó versenyzést kívánunk!

1. feladat 2 pont

A 6.1.52 kernel verziót futtató Linux rendszeren az alábbi systemd konfiguráció található:

`[Unit]``Description=Simple service to test memory limit.``[Service]``ExecStart=/root/memory_test``MemoryHigh=1M``[Install]``WantedBy=multi-user.target`

Mi történik, ha a megadott folyamat átlépi az 1M memória alokációt?

Válasz

- ☐ A cgroup meghívja az OOMkiller-t -TERM szignállal
- ☐ A cgroup meghívja az OOMkiller-t -KILL szignállal
- ☐ A cgroup nem hívja meg az OOMKiller-t, de erős memória visszavonási kényszereket alkalmaz

2. feladat 0 pont

Szeretnénk a 1234 id-vel rendelkező folyamatnak elsőbbséget adni az I/O műveletekhez és az sda tároló eszközhöz.

```
CONFIG_CGROUPS=y
CONFIG_BLK_CGROUP=y
CONFIG_CGROUP_WRITEBACK=y
CONFIG_CGROUP_SCHED=y
CONFIG_CGROUP_PIDS=y
CONFIG_CGROUP_RDMA=y
CONFIG_CGROUP_FREEZER=y
CONFIG_CGROUP_HUGETLB=y
CONFIG_CGROUP_DEVICE=y
CONFIG_CGROUP_CPUACCT=y
CONFIG_CGROUP_PERF=y
CONFIG_CGROUP_BPF=y
CONFIG_CGROUP_MISC=y
CONFIG_SOCK_CGROUP_DATA=y
CONFIG_BLK_CGROUP_RWSTAT=y
CONFIG_BLK_CGROUP_PUNT_BIO=y
CONFIG_BLK_CGROUP_IOLATENCY=y
CONFIG_BLK_CGROUP_FC_APPID=y
CONFIG_BLK_CGROUP_IOCOST=y
CONFIG_BLK_CGROUP_IOPRIO=y
CONFIG_NETFILTER_XT_MATCH_CGROUP=m
CONFIG_NET_CLS_CGROUP=m
CONFIG_CGROUP_NET_PRIO=y
CONFIG_CGROUP_NET_CLASSID=y
```

konfigurációs paraméterekkel rendelkezik.

A következő:

```
cgroup2 /sys/fs/cgroup cgroup2 rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_r
```

csatolási pont létezik. És ezen az elérési útvonal alatt található fájlok:

```
/sys/fs/cgroup/io-group/cgroup.controllers
```

```
cpu io memory pids
```

```
/sys/fs/cgroup/io-group/cgroup.subtree_control
```

```
io
```

```
/sys/fs/cgroup/io-group/fast/io.bfq.weight
```

```
default 500
```

adatot tartalmaznak. Illetve az sda tárolóeszközön az ütemezőnek a következő:

```
/sys/block/sda/queue/scheduler
```

```
none mq-deadline kyber [bfq]
```

beállítását választottuk ki.

Milyen paranccsal tudjuk elérni a célunkat ezen feltételek esetén?

Válasz

☐

```
echo 1234 > /sys/fs/cgroup/io-group/cgroup.proc
```

☐

```
echo 0::/io-group/fast > /proc/1234/cgroup
```

☐

egyikkel sem az előzőek közül

3. feladat 1 pont

Szeretnénk, hogy amikor a 6.6.0 verziójú Linux kernel nem képes az egyik folyamat memória allokáció kérelmét teljesíteni, a normál működés folytatása érdekében a futó folyamatok közül az egyiket állítsa le. Ezzel próbáljon a

használatban lévő memóriából felszabadítani. Milyen kernel paraméterekkel tudjuk ezt a viselkedést elérni, úgy hogy a kernel korlátozza a megengedett memória mennyiségét, ami túlfoglalható?

Válasz



```
vm.oom_kill_allocating_task = 0
vm.overcommit_kbytes = 0
vm.overcommit_memory = 2
vm.overcommit_ratio = 50
vm.panic_on_oom = 0
```



```
vm.oom_kill_allocating_task = 0
vm.overcommit_kbytes = 1024
vm.overcommit_memory = 1
vm.overcommit_ratio = 0
vm.panic_on_oom = 0
```



```
vm.oom_kill_allocating_task = 1
vm.overcommit_kbytes = 0
vm.overcommit_memory = 0
vm.overcommit_ratio = 50
vm.panic_on_oom = 0
```



```
vm.oom_kill_allocating_task = 0
vm.overcommit_kbytes = 0
vm.overcommit_memory = 0
vm.overcommit_ratio = 50
vm.panic_on_oom = 0
```

4. feladat 1 pont

Mi az alapvető különbség az AppArmor és SELinux között? Mindkettő kötelező hozzáférés-ellenőrzés (MAC) biztonsági keretrendszer a Linux számára.

Válasz



Az AppArmor útvonal alapú megközelítést alkalmaz, míg a SELinux címkézés alapút.

- ☐ Az AppArmor a felhasználó szintű biztonságra összpontosít, míg a SELinux elsősorban a kernel szintű biztonságot felelős.
- ☐ Az AppArmor több platformos támogatásra van tervezve, míg a SELinux a Red Hat alapú disztribúciókhoz specifikus.
- ☐ Az AppArmor és a SELinux között nincsenek alapvető különbségek. Ugyan azt a célt szolgálják.

5. feladat 3 pont

Másik csapat által lefejlesztett démonhoz szükséges jogok kivitelezésének egy feladatát kell megterveznünk egy RHEL 8.5 OS-en, ami SELinux enforced módban fut.

A megkapott dokumentáció alapján a démon telepítési könyvtára alatti hozzáféréseket és címkéket az igényeknek megfelelően kialakították már. Ezen felül kell lehetővé tennünk a /www/data olvasását, /www/tmp írását és olvasását, valamint a 443 tcp port hallgatását a démon számára. Továbbá kikötötték, hogy kizárólag a démon jelen állapotában a működéshez feltétlen szükséges módosításokat végezhetjük csak el a rendszeren.

Az alábbi parancsok kimenetelét bocsátották rendelkezésünkre:

```
[root@node1 ~]# systemctl cat mydaemon.service
# /usr/lib/systemd/system/mydaemon.service
[Unit]
Description=System Logger Daemon
Conflicts=emergency.service emergency.target
After=network-online.target
[Service]
User=mydaemonuser
Group=mydaemonuser
AmbientCapabilities=CAP_NET_BIND_SERVICE
Type=notify
ExecStart=/opt/mydaemon/sbin/mydaemon -w
ExecReload=/bin/kill -HUP $MAINPID
StandardOutput=journal
StandardError=journal
Restart=on-failure
UMask=0027
WorkingDirectory=/opt/mydaemon/
[Install]
WantedBy=multi-user.target
```

```
[root@node1 ~]# ps auxfZ
```

```
....
```

```
system_u:system_r:unconfined_service_t:s0 mydaemonuser 1563 4.1 8.1 89704 2204
system_u:system_r:unconfined_service_t:s0 mydaemonuser 1566 0.6 1.5 89876 4072
system_u:system_r:unconfined_service_t:s0 mydaemonuser 4935 0.5 1.2 89808 4052
```

```
...
```

```
[root@node1 ~]# semanage port -l | grep 443
```

```
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 900
```

```
[root@node1 ~]# sesearch -A -s mydaemon_t | grep http_port_t
```

```
[root@node1 ~]#
```

```
[root@node1 ~]# semanage fcontext -l | grep ^/www
```

```
[root@node1 ~]#
```

```
[root@node1 ~]# semanage fcontext -l | grep ^/opt/mydaemon/opt/mydaemon(/.*)?
```

```
[root@node1 ~]# ls -alZ /opt/mydaemon
```

```
drwxr-xr-x. 10 root root system_u:object_r:mydaemon_t:s0      105 Jul 26
drwxr-xr-x.  3 root root system_u:object_r:usr_t:s0          23 Jul 26
drwxr-xr-x.  2 root root system_u:object_r:mydaemon_t:s0     4096 Jul 26
drwxr-xr-x.  3 root root system_u:object_r:mydaemon_t:s0      112 Jul 26
drwxr-xr-x.  6 root root system_u:object_r:mydaemon_t:s0      214 Jul 26
drwxr-xr-x. 10 root root system_u:object_r:mydaemon_t:s0    12288 Jul 26
drwxr-xr-x.  2 root root system_u:object_r:mydaemon_t:s0       78 Jul 26
drwxr-xr-x.  7 root root system_u:object_r:mydaemon_t:s0       72 Jul 26
drwxr-xr-x.  3 root root system_u:object_r:mydaemon_var_t:s0   42 Jul 26
```

```
[root@node1 ~]# ls -alZ /www
```

```
ls: cannot access '/www': No such file or directory
```

Válasz

```
mkdir /www /www/tmp /www/data
chown -R root:mydaemonuser /www
chmod -R 750 /www
chmod 770 /www/tmp
```

```
mkdir /www /www/tmp /www/data
chown -R root:mydaemonuser /www
chmod -R 750 /www
chmod 770 /www/tmp
semanage port -a -t mydaemon_port_t -p tcp 443
```

```
mkdir /www /www/tmp /www/data
chown -R root:mydaemonuser /www
chmod -R 750 /www
chmod 770 /www/tmp
semanage fcontext -a -t mydaemon_t '/www(/.*)?'
restorecon -Rv /www
```

```
mkdir /www /www/tmp /www/data
chown -R root:mydaemonuser /www
chmod -R 750 /www
chmod 770 /www/tmp
semanage port -m -t mydaemon_port_t -p tcp 443
semanage fcontext -a -t mydaemon_t '/www(/.*)?'
restorecon -Rv /www
```

```
mkdir /www /www/tmp /www/data
chown -R root:mydaemonuser /www
chmod -R 750 /www
chmod 770 /www/tmp
semanage port -a -t mydaemon_port_t -p tcp 443
semanage fcontext -a -t mydaemon_t '/www/*'
restorecon -Rv /www
```


Megoldások beküldése