Red Book: Astra Linux Common Edition 2.12

- Astra Linux Common Edition 2.12
-
-
-

Astra Linux Common Edition 2.12

1. - - ()
2. "" BIOS .

   P.S.

   "" :

   - 8 ;
   - ( );
   - , .

3. "" "" ".
   , , , , "" - .
4. (, , .).
   (WiFi, Bluetooth).
   WiFi - VPN.
5. Intel Execute Disable Bit (XD-Bit) AMD No Execute Bit (NX-Bit) .
6. " " ILO, RSA, iDRAC, ThinkServer EasyManage, AMT, iMana - , , , IP KVM.
7. (, , BIOS .). BIOS , , , ...
8. ( ),
   ,

1.

	/
/	(, /boot). ext4.
/boot	. ext2, ext3, ext4.
/home	. ext4. `noexec,nodev,nosuid`.
/tmp	. ext4. `noexec,nodev,nosuid`.
/var/tmp	. ext4. `noexec,nodev,nosuid`.
swap	. .

, /tmp 250 .

2. */home /tmp /var/tmp* `noexec,nodev,nosuid`
3. " ":
   a. hardened. hardened lkrg generic (. astra-safepolicy);
   b. ;
   c. ;
   d. ufw;
   e. ulimits;
   f. ptrace;
   g. ;
   h. sudo ;

1. , ;
2. "" Grub. , Intel, ;
3. HARDENED, , ;
4. , Intel Management Engine (MEI). ;
5. Astra Linux:

   Astra Linux Common Edition : https://download.astralinux.ru/astra/current/orel/repository/

   , , :

   sudo apt update && sudo apt upgrade

6. astra-safepolicy:

```
sudo apt install astra-safepolicy
```

7. /boot , `ro` (`rw`);
8. secureboot (usb-flash astra-secureboot, , , BIOS) ;
9. , . astra-safepolicy, :

```
sudo astra-console-lock enable
```

   fly-admin-smc.

   astra-console;

10. , . astra-safepolicy, :

```
sudo astra-interpreters-lock enable
```

    fly-admin-smc;

11. , astra-macros-lock:

```
astra-macros-lock enable
```

    fly-admin-smc;
12. ptrace, :

```
astra-ptrace-lock enable
```

fly-admin-smc;

13. , , ;
14. , ;
15. , VPN ( );
16. , GPG- Thunderbird Enigmail ( );
17. "" .

> **P.S.**
>
> "" -
>
> - 8 ;
> - ( );
> - , .

18. , pam_tally ( );
19. fly-admin-smc;
20. (ulimits), :

```
sudo astra-ulimits-control enable
```

fly-admin-smc;

21. (..) :

```
systemdgenie
```

22. ufw, .
iptables , : ,

```
- iptables
- ufw
- gufw
```

23. fly-admin-smc .conf */etc/sysctl.d:*

```
fs.suid_dumpable=0
kernel.randomize_va_space=2
kernel.sysrq=0
net.ipv4.ip_forward=0
net.ipv4.conf.all.send_redirects=0
net.ipv4.conf.default.send_redirects=0
```

, , .
:

```
sudo sysctl -a | more
```

24. python :

```
find /usr/lib/python* -type f -name "_ctype*" -exec sudo dpkg-
statoverride --update --add root root 640 {} \;
```

25. , ,
.

26. , , :

```
sudo astra-mount-lock
```

fly-admin-smc;

27. . , .

28. fail2ban.

29. sudo:

```
sudo astra-sudo-control enable
```

, , , /etc/sudoers

Defaults timestamp_timeout=0

/etc/sudoers :

```
sudo visudo
```

- sudo /etc/pam.d/sudo:

```
account required pam_tally.so
```

/etc/pam.d/sudo:

```
@include common-auth
@include common-account
@include common-session
account required pam_tally.so
```

. sudo