Settings, guides

- How to Improve CSF Performance Using ipset
- How to Archive Old Content on Your Server
- How to Count Inodes per File and Directory in Linux
- How to Force Restart a Linux Server Safely
- How to Create a Database Backup
- How to Choose the Right DNS Resolver for a VPS
- How to Fix a VPS That Does Not Boot After a Kernel Update
- How to Set a PTR Record (Reverse DNS Setup)
- How to Order a New VPS Server
- How to Install and Configure CSF Firewall

How to Improve CSF Performance Using ipset

For servers where the CSF firewall is running slowly using iptables, or may stop when large amounts of IP addresses are configured between iptables rules. This problem can be solved quickly by installing ipset.

Ipset is a framework that belongs to the Linux kernel. Allows you to store combinations of IP addresses, networks, TCP / UDP ports, and MAC addresses. The data stored in the IP set is quickly accessible and can be searched and updated without reloading iptables.

To configure, you must install the ipset package that can be used by users using CentOS, Red Hat, and Fedora (yum) OS by issuing the following command:

```
sudo yum install ipset -y
```

If you are using an apt-based Linux distribution such as Ubuntu, or Debian, you must issue the following command:

```
sudo apt-get install ipset -y
```

After installing ipset and related dependencies, ipset must be enabled in the CSF configuration file, which can be done by modifying the main configuration file:

```
nano /etc/csf/csf.conf
```

After opening, locate the `lf_ipset` line and make the change. To search, press `CTRL+W`, and then type `lf_ipset`, and then press `enter`.

Change the value of `0` in `lf_ipset` to `1`. After the change, the configuration file will look like this:

```
LF_IPSET = "1"
```

Then save the changes and exit the nano editor by pressing the `CTRL+X` keys, and then press the `Y` key and finally `enter`.

As a last step, restart the CSF and LFD services to validate the changes

```
csf -r
```

How to Archive Old Content on Your Server

This tutorial can help you compress or restore previous unused web content.

If for some reason the developer of the previous website is not available, the server’s previous website code can be found, then it should be saved and saved and removed from the server. Because the source code for old web pages is usually not updated, it is likely to improve vulnerability and vulnerability. By taking advantage of this, they can load harmful codes that can be used to send out, for example, spam.

Therefore, we recommend that you archive the contents of the old site as soon as possible and then remove it from the server. Because the source code of the pages may be large and may contain many files, it is advisable to compress the affected folder, such as gzip. If you want to keep the old page content compressed on the server, it is recommended that you specify a directory that is not accessible from the web. For example, /var/www/oldwebpage.tar.gz

COMPRESS A FOLDER

After you connect to the server via SSH, you can create a backup by issuing the following command:

```
tar -czvf public_html_backup.tar.gz public_html/
```

EXTRACT AN ARCHIVE

`tar` is the program that performs compression, using the `-c` switch to create the archive. The `-z` switch calls gzip for compression, using the `-v` option to set the verbose output that displays the compression process on the current console. The `-f` option allows you to specify the archive name, which in this case is `public_html_backup.tar.gz`, which can of course be freely modified, but the `.tar.gz` extension must be kept in the file name. The last parameter `public_html/` which is the directory whose content you want to compress is recursive by default, so all files and subdirectories will be found in the archive.

To decompress, use the following command:

```
tar -xzvf public_html_backup.tar.gz -C /public_html_backup
```

After the `-C` switch, you can specify the folder name in which you want to restore the contents of the archive concerned.

How to Count Inodes per File and Directory in Linux

Occasionally, you may not be aware of the amount of free space on the server during server operation. How much and what kind of data the libraries store.

For example, if you are curious about the number of files and folders (inodes) recursively in each folder under the public_html folder, enter the following command:

```
find -xdev -printf '%h\n' | sort | uniq -c | sort -k 1 -n
```

Depending on the number of folders or files, the run of the issued command will display the data in a shorter time, please be patient.

How to Force Restart a Linux Server Safely

Occasionally, some devices are locked, multiple disk mountings are lost, or the processes are stuck and the server responds very slowly. In such cases, the easiest solution is to restart the server.

For example, if one of the devices is locked or a mount point is damaged, the server cannot be restarted in the normal way.

> **Attention!** The following command is not safe to use, so use it only in very justified cases! Adding a command can damage the file system and cause data loss.

After connecting to the server via SSH, you can force restart by issuing the following command:

```
echo 1 > /proc/sys/kernel/sysrq && echo b > /proc/sysrq-trigger
```

> **Attention!** You cannot undo the release of this command!

The above command allows `sysrq` to be used. This allows us to communicate directly with the kernel. The second step sends the trigger `b` (to restart) to sysrq, which forces a restart.

The system will restart within a few minutes approximately as if the reset button was pressed on the machine. After restarting the system, you will be able to find and fix the problem.

How to Create a Database Backup

Almost every modern website uses a MySQL database. More popular content management systems, such as WordPress, Magento, Joomla, store all data in a MySQL database. If, for some reason, we want to back up the database, such as a MySQL server update, then it is possible to extract the data stored in the database or to recover the dump in case of a possible error.

COMPRESS A FOLDER

After you connect to the server via SSH, you can create a backup by issuing the following command:

```
mysqldump -u user_name -p database_name --single-transaction | gzip -2 > db.sql.gz
```

By issuing the above command, you create a compressed dump with a single transaction token.

> Of course, it is also possible to make an uncompressed dump, but it will take a lot more time and more space will be spent on dumped content.

```
mysqldump -u user_name -p database_name > db.sql
```

EXTRACT AN ARCHIVE

You can do this by issuing the following command

```
gunzip < db.sql.gz | mysql -u user_name -p database_name
```

To restore an uncompressed database, use the following command:

```
mysql -u user_name -p database_name < db.sql
```

How to Choose the Right DNS Resolver for a VPS

Customers often ask us what DNS resolvers we recommend to use. However, it is not easy to answer this question if we consider the performance/uptime. We can now recommend using the following resolvers:

GOOGLE PUBLIC DNS

- 8.8.8.8
- 8.8.4.4
- 2001:4860:4860::8888
- 2001:4860:4860::8844

NTT

- 129.250.35.250
- 129.250.35.251
- 2001:418:3ff::53
- 2001:418:3ff::1:53

VERISIGN PUBLIC DNS

- 64.6.64.6
- 64.6.65.6
- 2620:74:1b::1:1
- 2620:74:1c::2:2

LEVEL 3

- 4.2.2.2
- 4.2.2.4

How to Fix a VPS That Does Not Boot After a Kernel Update

Issue

Upgrading kernel(s) inside Linux guests to the following versions will break them. Updated guest(s) won’t ever boot and will crash on startup.

Environment

CentOS 6.x kernel version >= 2.6.32-754.2.1.el6.x86_64

Debian 9.x kernel version >= 4.9.0-7-amd64

Resolution

The issue can be fixed in one of the following ways:

1. Skip the recent kernel while updating guest’s packages:
   - Update CentOS 6.x with:

     ```
     # yum update --exclude=kernel*2.6.32-754.2.1*
     ```

   - Update Debian 9.x with:

     ```
     # apt-mark hold linux-image-amd64 linux-headers-amd64
     # apt-get update
     # apt-get dist-upgrade
     ```

2. After the kernel was updated, add the following kernel options to the GRUB boot loader configuration file:
   - For CentOS 6.x, add *eagerfpu=off* option to *edit /boot/grub/grub.conf* file
   - For Debian 9.x, add *elevator=noop* and *pti=off* options to *edit /boot/grub/menu.lst* file.

How to Set a PTR Record (Reverse DNS Setup)

You can also set the PTR record, please follow these steps:

- Log in at https://admin.dotroll.com and then click **Services** / **My Services**.
- Click the **Active** button on the services line and then the **Manage** button in the middle of the page on the **Server Information** tab.
- After loading the page, click the **Network** tab at the bottom of the page
- Select the IP address you want to edit, and then click **[Edit]** in the **Reverse DNS** column.
- In the popup window that appears, enter the desired name and click the **Update** button.

> **Important notice:**
> The user interface can only set the reverse value, if before you have assigned a type A (or IPv6 address type AAAA) record for the VPS IP address.

How to Order a New VPS Server

To use Dotroll Virtual Private Server (VPS), you must have an account payer account. If you don’t already have one, you can create one here.

After the login, you can start the order in the Order -> Virtual Server menu.

Steps for ordering:

1. First, select the architecture.
2. Then select the operating system type.
3. After selecting the operating system, it is possible to select a version within the distribution and then specify the number of resource units.
4. You must then enter the administrator password.

How to Install and Configure CSF Firewall

Ebben a cikkben elmagyarázzuk, hogyan telepíthető és konfigurálható a ConfigServer Security & Firewall-t (rövidítve a CSF). A CSF egy teljes körű biztonsági csomag, amit használhat tűzfal és behatolás / bejelentkezési hiba észlelő rendszerként.

INSTALLING AND CONFIGURING CSF IN LINUX

Ahhoz, hogy a CSF telepíthető legyen és normális módon fusson a Perl és a libwww csomagoknak telepítve kell lenniük a szerveren. A CSF-et jelenleg bármelyik RHEL, CentOS, openSUSE, Debian és Ubuntu disztribúció alá lehet telepíteni.

```
yum install perl-libwww-perl
apt install libwww-perl
```

1. **Download CSF**

   ```
   cd /usr/src
   wget https://download.configserver.com/csf.tgz
   ```

2. **Extract the CSF tarball**

   ```
   tar xzf csf.tgz
   cd csf
   ```

3. **Run the CSF Installation Script**A folyamat ezen része ellenőrzi, hogy az összes függőség telepítve van-e, létre hozza a webes felülethez szükséges könyvtárstruktúrákat és fájlokat, észleli az éppen megnyitott portokat, valamint figyelmezteti Önt arra, hogy a csf és az lfd démonokat újra kell indítani, miután elvégezte a kezdeti beállítást.

   ```
   sh install.sh
   perl /usr/local/csf/bin/csftest.pl
   ```

   A fenti parancs várható kimenete a következő:

```
Testing ip_tables/iptable_filter...OK
Testing ipt_LOG...OK
Testing ipt_multiport/xt_multiport...OK
Testing ipt_REJECT...OK
Testing ipt_state/xt_state...OK
Testing ipt_limit/xt_limit...OK
Testing ipt_recent...OK
Testing xt_connlimit...OK
Testing ipt_owner/xt_owner...OK
Testing iptable_nat/ipt_REDIRECT...OK
Testing iptable_nat/ipt_DNAT...OK

RESULT: csf should function on this server
```

4. **Disable Firewall and Configure CSF**Állítsa le, majd tiltsa le a firewalld-t a következő parancsok kiadásával, ezt követően állítsa be a CSF-et.

```
systemctl stop firewalld
systemctl disable firewalld
```

Az `/etc/csf/csf.conf` fájlban módosítsa a `TESTING = "1"` változó értékét `TESTING = "0"`-ra különben az lfd démon nem indul el), ezt követően állítsa be a vesszővel elválasztva a bejövő és kimenő portokat (TCP_IN és TCP_OUT). A fájl tartalma megközelítőlegesen így kell hogy kinézzen:

```
# Testing flag - enables a CRON job that clears iptables incase of
# configuration problems when you start csf. This should be enabled until you
# are sure that the firewall works - i.e. incase you get locked out of your
# server! Then do remember to set it to 0 and restart csf when you're sure
# everything is OK. Stopping csf will remove the line from /etc/crontab
#
# lfd will not start while this is enabled
TESTING = "0"

# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"

# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,53,80,110,113,443,587,993,995"
```

A megfelelő beállítások megadását követően mentse el a fájlt, majd lépjen ki a szerkesztőből.

5. **Restart and Test CSF**

```
# systemctl restart {csf,lfd}
# systemctl enable {csf,lfd}
# systemctl is-active {csf,lfd}
# csf -v
```

Innentől a CSF már használatra kész, azonban a tűzfal és behatolásérzékelés szabályait még célszerű beállítani.

USEFULL CSF COMMANDS

A jelenlegi tűzfal szabályok kilistázásához adjuk ki a következő parancsot:

```
# csf -l
```

A tűzfal szabályokat a következő parancs segítségével törölheti:

```
# csf -f
```

A tűzfal szabályokat a következő parancs segítségével töltheti újra:

```
# csf -r
```

A fenti parancsokat lehetőség szerint jegyezze meg mert a későbbiek során szüksége lehet rájuk amikor a **csf** és az **lfd** újraindításra kerül.

ALLOWING AND FORBIDDING IP ADDRESSES

A bejövő kapcsolatok engedélyezése 192.168.0.10-től.

```
# csf -a 192.168.0.10
```

Hasonlóképpen megtagadhatja a 192.168.0.11-ből származó kapcsolatokat.

```
# csf -d 192.168.0.11
```

Eltávolíthatja a fenti szabályokat, ha ezt szeretné.

```
# csf -ar 192.168.0.10
# csf -dr 192.168.0.11
```

A `-ar` illetve a `-dr` kapcsolók használata a fenti IP-címmel társított meglévő engedélyezési és megtagadási szabályokat eltávolítja.

LIMITING INCOMING CONNECTIONS BY SOURCE

A kiszolgáló tervezett felhasználásától függően a kapcsolatokat korlátozhatja port alapon, és a beérkező próbálkozások száma szerint. Ehhez nyissa meg az `/etc/csf/csf.conf` fájlt, és keresse meg a `CONNLIMIT` részt. Megadható több port, a portokat `;` elválasztva adja meg. Például:

```
CONNLIMIT = "22; 2,80; 10"
```

a fenti példában csak 2 bejövő kapcsolatot engedélyez ugyanabból a forrásból a 22-es portra, míg a 80-as TCP port esetén egy IP címről maximum 10 kapcsolatot engedélyez.

SENDING ALERTS VIA EMAIL

Számos riasztási típus beállítható, ehhez keresse meg az `EMAIL_ALERT` részt a `/etc/csf/csf.conf` fájlban, majd ellenőrizze le hogy az értéke `1`-re van e állítva. Például:

```
LF_SSH_EMAIL_ALERT = "1"
LF_SU_EMAIL_ALERT = "1"
```

az `LF_ALERT_TO` résznél megadott email címre küldi minden egyes alkalommal, amikor valaki sikeresen bejelentkezik az SSH-n keresztül, vagy átvált egy másik fiókra a `su` parancs segítségével.

CSF CONFIGURATION FILES

A következő fájlok segítségével módosítható a `csf` működése. A `csf` összes konfigurációs fájlja a `/etc/csf` könyvtár alatt található. Az alábbi fájlok módosítása esetén a `csf démont újra kell indítani.`

- **csf.conf**: A CSF fő konfigurációs állománya.
- **csf.allow**: A tűzfalon engedélyezett IP és CIDR címek listája.
- **csf.deny**: A tűzfalon található tiltott IP és CIDR címek listája.
- **csf.ignore**: A tűzfalon a figyelmen kívül hagyott IP és CIDR címek listája.
- **csf.*ignore**: A tűzfalon a figyelmen kívül hagyott egyéb felhasználók, fájlok, IP címek listája.

REMOVE CSF

Ha teljesen el szeretné távolítani a CSF-et, akkor futtassa a `/etc/csf/uninstall.sh`

```
#/etc/csf/uninstall.sh
```

A fenti parancs teljesen törli a CSF-et az összes fájlt és mappát.