GUIDE

STORMSHIELD LOG SUPERVISOR

UPDATE GUIDE

Versions 1 and 2

Document last updated: July 22, 2024

Reference: sls-en_update_gde

Table of contents

Change log

Date	Description
July 22, 2024	Fixes two SLS configuration paths in section "Updating SLS from version 1.1.1 to 2.0.0"
July 4, 2024	New document

Getting started

Welcome to the SLS Update Guide.

To update your SLS to a newer version, we recommend that you carefully follow this guide.

Before updating SLS, be sure to:

- Read the following documents:
  - The Product life cycle Log Supervisor guide.
    SLS versions are divided into major, minor and corrective versions. For more information about the SLS Life Cycle management policy and SLS compatibilities, refer to this guide. If a version has several patch versions, always choose the most recent so that you benefit from the latest functional patches and bug fixes.
  - The SLS Release Notes to find out what the SLS versions contain.
- Back up SLS by creating a snapshot of the virtual machine so that you can restore it if necessary.

In this document, Stormshield Log Supervisor is referred to in its short form SLS.

NOTE
This document covers the update of an existing SLS. Specific deployment guides are available for a new SLS installation.

Patch dependencies

To update SLS, you need the update file (*.pak*) of the corresponding version. In SLS, an update file is called a patch.

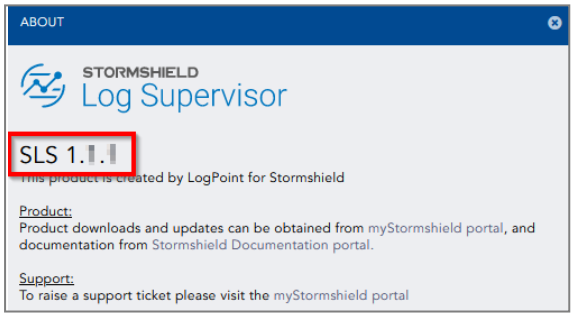
Depending on your current SLS version, you may need to install one or more intermediate patches:

Version / Patch	Can be installed on
2.0.0	1.1.1
1.1.1	1.1.0
1.1.0	1.0.0

To determine which version of SLS is currently installed:

- For SLS version 1, click on the Stormshield Log Supervisor logo in the top banner,
- For SLS version 2, click on ⓘ **Help** > **About SLS** in the navigation bar on the left.

SLS version 1



SLS version 2

Downloading an SLS patch

1. In your MyStormshield personal area, go to **Downloads** > **Downloads**.
2. Select **Stormshield Log Supervisor** from the suggested categories.
3. Download the SLS patch (*.pak* file) you want by clicking on its name. If you need to install multiple patches due to patch dependencies, download them all now.
4. You can check the integrity of the downloaded file:
    1. Run one of the following commands:
        - Linux: *sha256sum <filename>*
        - Windows: *CertUtil -hashfile <filename> SHA256*
    2. Compare the result with the hash indicated in the MyStormshield interface. To view it, click on **Display** in the **SHA256** column of the file in question.

Updating SLS

Use the following procedures to update SLS to version 2.0.0, 1.1.1 or 1.1.0. Check the patch dependencies and be sure to apply all intermediate patches.

From version 1.1.1 to 2.0.0

IMPORTANT
It is strongly recommended that you back up your SLS before starting this update procedure.

Specific patch installation requirements

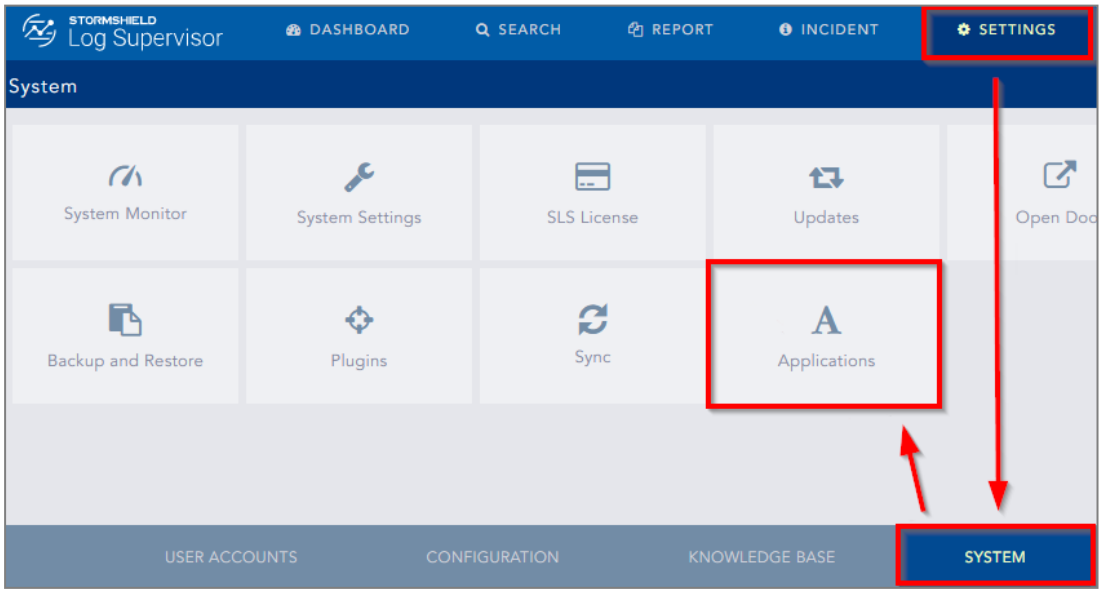
- CPU: 8-core minimum
- RAM: 16GB minimum
- Minimum disk space required:
  - 500MB in */tmp*
  - 15GB in */opt*
  - 32GB in */opt/makalu/storage*

  To check the available disk space, go to **Settings >> System >> System Monitor** and click **Disk Usage**. If you need to increase the disk size, refer to the appendix Extending disk size with an added disk.

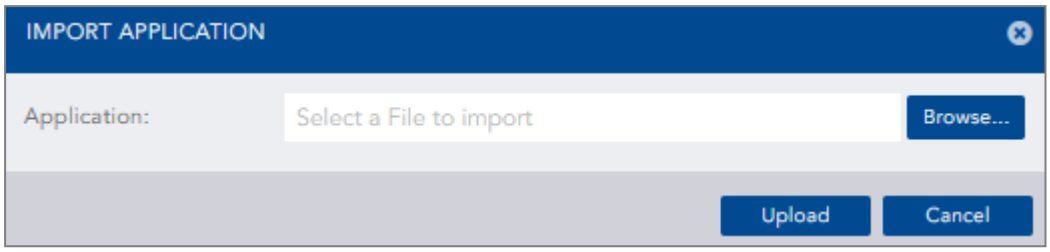
Install the SLS Upgrade Helper

You must install the SLS Upgrade Helper version 1.0.0 **before** you upload the 2.0.0 patch. It changes the SLS patch installation path from */tmp* to */opt/immune/storage/tmp*.

1. Download the SLS Upgrade Helper file (*SLSUpgradeHelper_1.0.0.pak*) from your MyStormshield personal area in **Downloads > Downloads > Stormshield Log Supervisor**.
2. On SLS, go to **Settings >> System >> Applications**.



3. Click **Import**.
4. Browse to the SLS Upgrade Helper *.pak* file and click **Upload**.

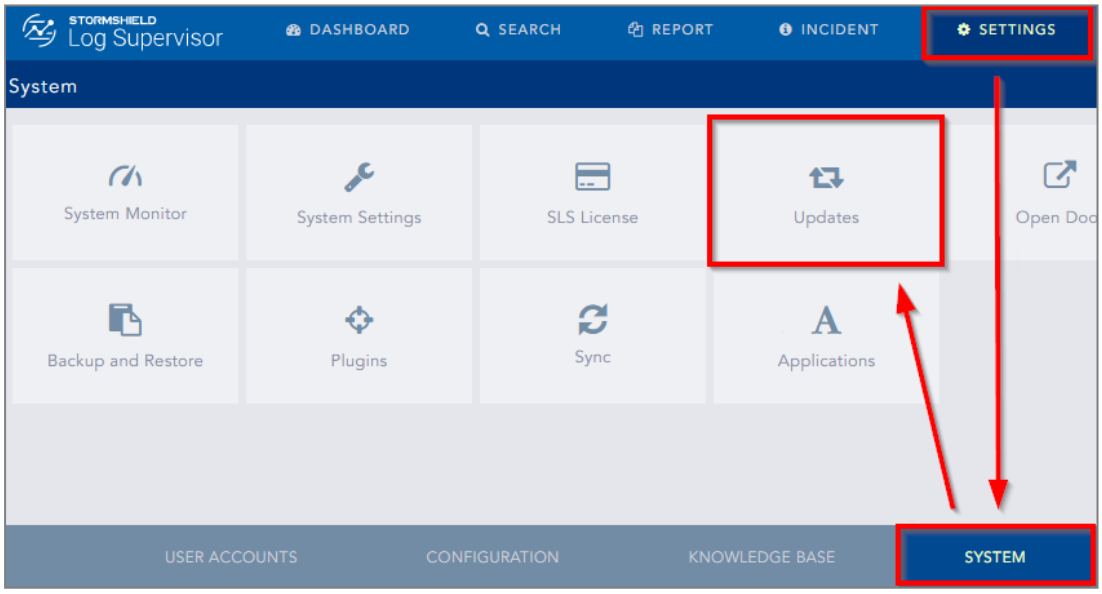


Install the SLS version 2.0.0 patch

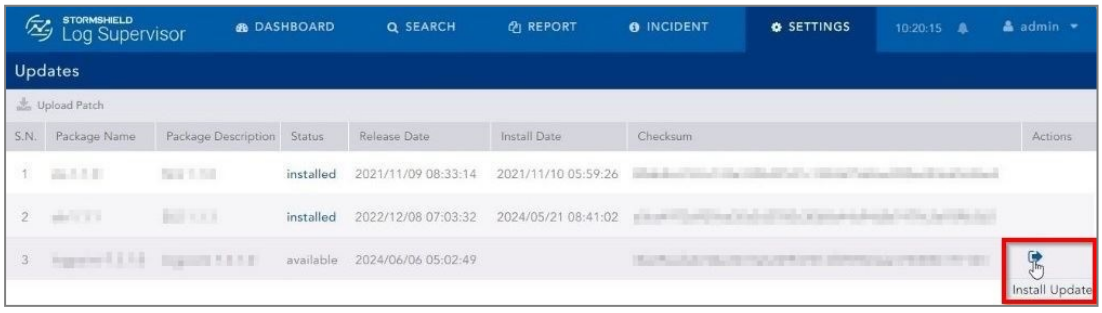
NOTE
The process may take some time:

- Depending on your network connection, you may experience a longer patch upload time as the patch size is 6.4GB,
- Depending on system load and available resources, the patch will take between 30 and 60 minutes to install on the system.

1. Download the SLS version 2.0.0 patch from your MyStormshield personal area.
2. On SLS, go to **Settings** >> **System** >> **Updates**.



3. Click **Upload Patch**. Browse for the downloaded *.pak* file and click **Upload**.
4. Click the **Install Update** icon from the **Actions** column.



5. Allow 30 to 60 minutes to complete the update. You can refresh the **Updates** page at any time to see if the update is complete. When completed, the machine restarts and the *Status* of the SLS patch is *installed*.

If the installation fails with one of the following error messages:

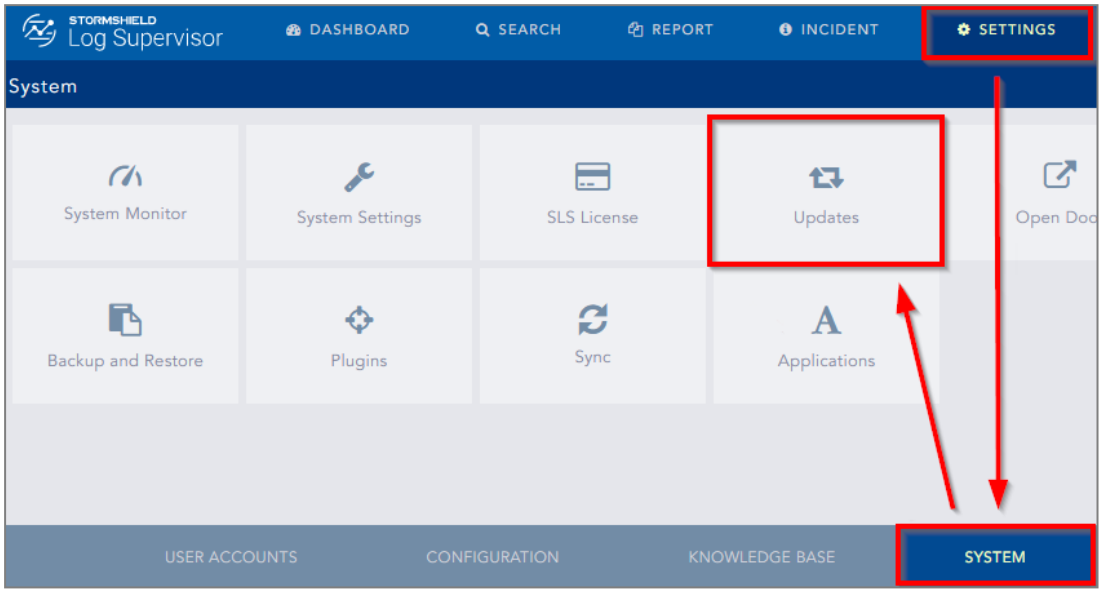
```
Precondition fail - /opt should have at least 7.0GB of free space
```

```
Precondition fail - /opt/makalu/storage should have at least 25GB of free
space
```

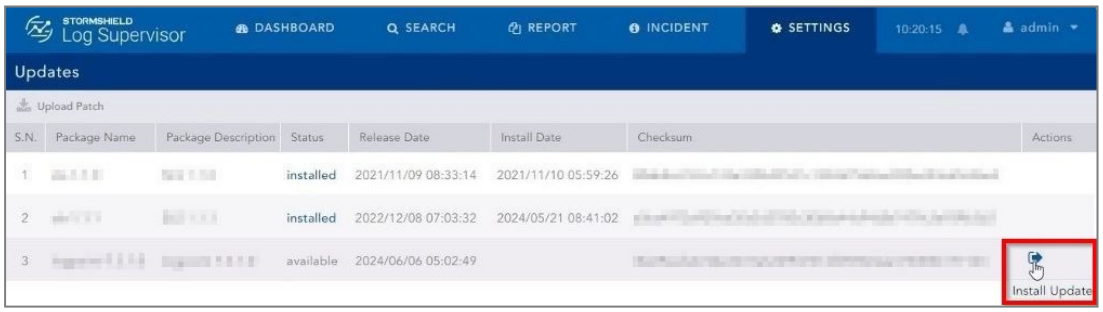
You must increase the disk size. For more information, refer to the appendix Extending disk size with an added disk.

From version 1.1.0 to 1.1.1

1. Download the SLS version 1.1.1 patch from your MyStormshield personal area.
2. On SLS, go to **Settings** >> **System** >> **Updates**.



3. Click **Upload Patch**. Browse for the downloaded *.pak* file and click **Upload**. Please wait a few minutes as the file may take some time to upload.
4. Click the **Install Update** icon from the **Actions** column.

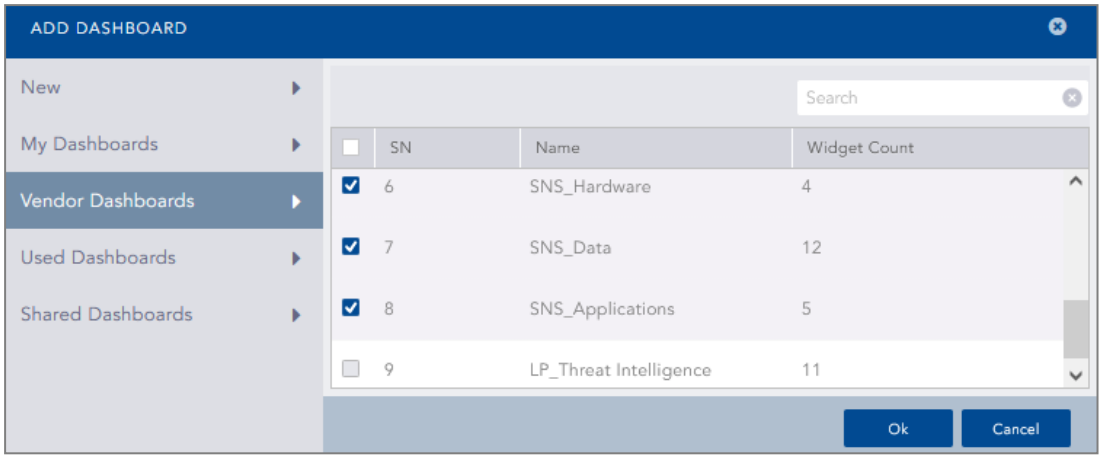


5. Wait a few moments for the update to end. Note that the **Install Logs** window does not notify you when the installation is complete. Go back to the **Updates** page to check that the *Status* of the SLS patch is *installed*.
6. To access the new version of SLS, log out from the user interface and then log in.

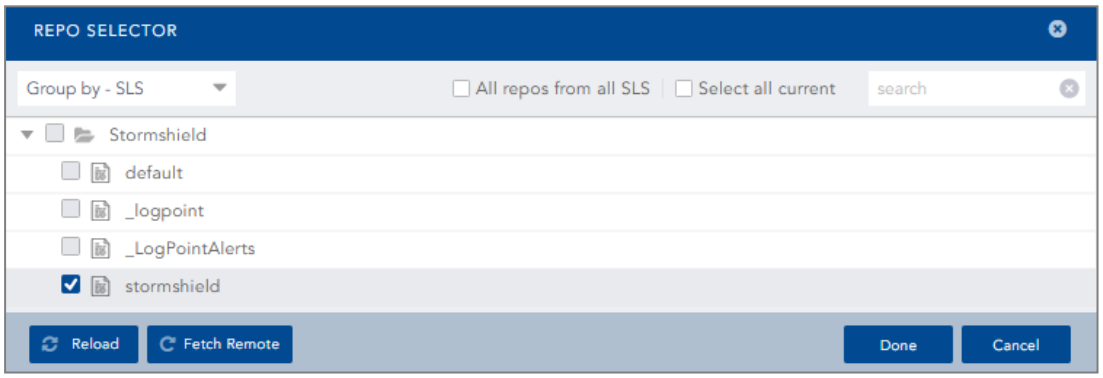
If you were using SNS built-in dashboards without any customization, you must manually remove the old dashboards and add the new ones:

1. Go to **Dashboard** from the navigation menu.
2. Remove all SNS dashboards by clicking the **Remove Dashboard** (✕) icon and clicking **Yes**.
3. Click the + icon to add the new dashboards and click **Vendor Dashboards**.

4. Select all **SNS** dashboards, and only SNS dashboards, then click **Ok**.



5. Select all **SNS** dashboards again, and click **Choose Repos**.
6. Unselect **Stormshield**, select **stormshield** (in lower case), then click **Done**.

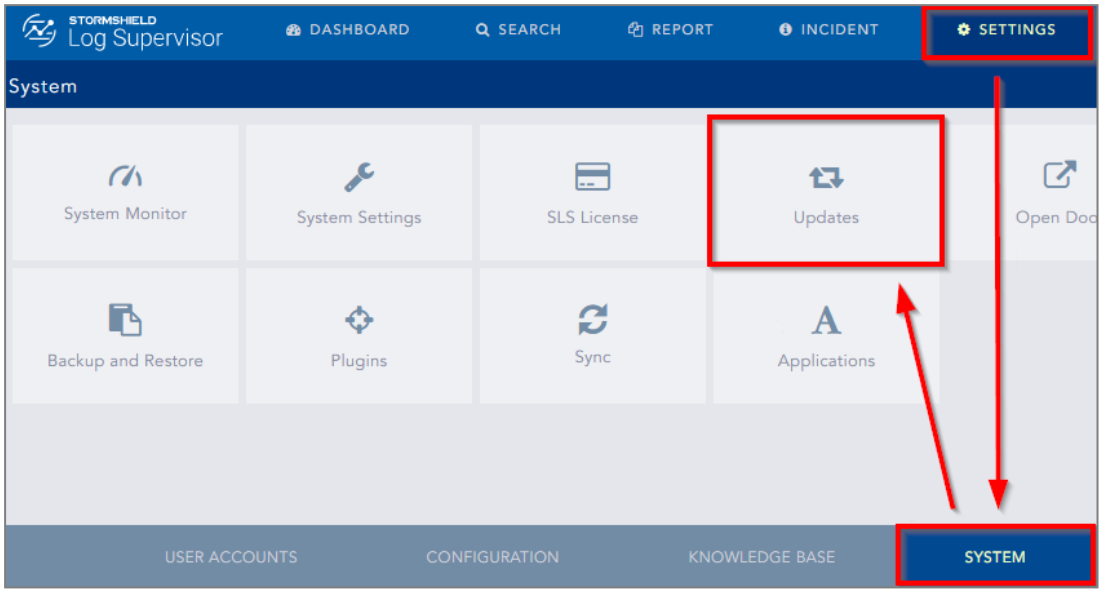


7. Click **Ok** to add the new dashboards.

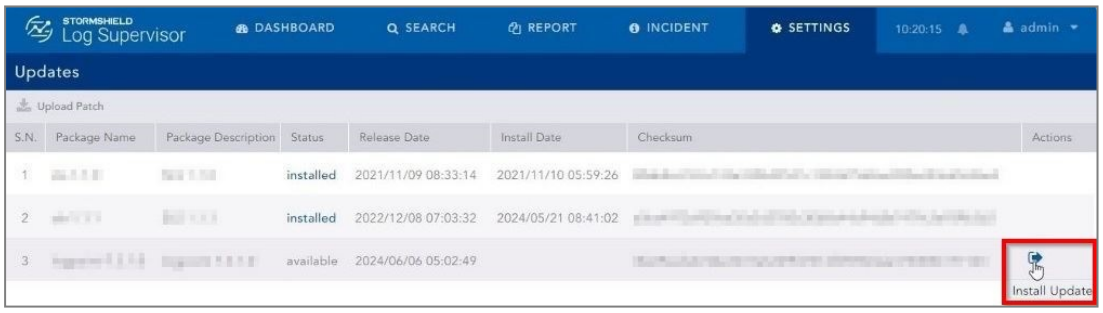
You can now update SLS to version 2.0.0.

From version 1.0.0 to 1.1.0

1. Download the SLS version 1.1.0 patch from your MyStormshield personal area.
2. On SLS, go to **Settings** >> **System** >> **Updates**.



3. Click **Upload Patch**. Browse for the downloaded *.pak* file and click **Upload**.
4. Click the **Install Update** icon from the **Actions** column.



5. Wait for the update to end. This takes several minutes. You can refresh the **Updates** page at any time to see if the update is complete. When completed, the machine restarts and the *Status* of the SLS patch is *installed*.
6. Refresh the page to access the new version of SLS.

You can now update SLS to version 1.1.1.

Further reading

Additional information and answers to questions you may have about SLS are available in the Stormshield knowledge base (authentication required).

Appendix: Extending disk size with an added disk

This appendix explains how to extend your disk size. You may need to do this if your SLS patch update fails due to insufficient disk space.

IMPORTANT
Effective management of disks and file systems is critical, as unintentional changes can result in data loss. Proceed at your own risk.

1. Log in to the SLS server CLI as a **li-admin** user.
2. Use the **lsblk** command to check the name of the newly added disk.

```
li-admin@LogPoint:~$ lsblk
NAME                 MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                    8:0    0  100G  0 disk
├─sda1                 8:1    0   30M  0 part
├─sda2                 8:2    0   18G  0 part /
├─sda3                 8:3    0  7.5G  0 part [SWAP]
└─sda4                 8:4    0 74.6G  0 part
├─LogPoint--vg-app  253:0    0 18.6G  0 lvm  /opt
└─LogPoint--vg-data 253:1    0 55.9G  0 lvm  /opt/makalu/storage
sdb                    8:16   0   10G  0 disk
```

Here, the new disk is **sdb**. Reboot the system if you can't see the new disk with the above command.

3. Check the size of the logical volume.

```
li-admin@LogPoint:~$ df -hT
Filesystem                     Type      Size  Used Avail Use% Mounted on
udev                           devtmpfs  3.9G     0  3.9G   0% /dev
tmpfs                          tmpfs     797M 1000K  796M   1% /run
/dev/sda2                      ext4       18G  9.0G  7.8G  54% /
tmpfs                          tmpfs     3.9G     0  3.9G   0% /dev/shm
tmpfs                          tmpfs     5.0M     0  5.0M   0% /run/lock
tmpfs                          tmpfs     3.9G     0  3.9G   0% /sys/fs/cgroup
/dev/mapper/LogPoint--vg-app   ext4       19G  2.8G   15G  17% /opt
/dev/mapper/LogPoint--vg-data  ext4       55G  509M   52G   1% /opt/makalu/storage
tmpfs                          tmpfs     797M  4.0K  797M   1% /run/user/1000
```

The current size of "**/dev/mapper/LogPoint--vg-app**" is 19GB.

The current size of "**/dev/mapper/LogPoint--vg-data**" is 55GB.

4. Format the new disk and create a partition on it:
   1. Format the new disk with the **gdisk** command. (*gdisk /dev/sdb* in this case).
   2. Enter **n** to add a new partition.
   3. Enter **1** as the partition number.
   4. Choose **First sector**. Press **Enter** for default value.
   5. Choose **Last sector**. Press **Enter** for default value.
   6. Choose **Hex code** *8e00* for Linux LVM.
   7. Then, press **p** to print new partition details.
   8. Press **w** to save the partition.
   9. Press **y** to confirm the partition creation.

```
li-admin@LogPoint:~$ gdisk /dev/sdb
GPT fdisk (gdisk) version 1.0.5

Partition table scan:
MBR: not present
BSD: not present
APM: not present
GPT: not present

Creating new GPT entries in memory.

Command (? for help): n
Partition number (1-128, default 1): 1
First sector (34-20971486, default = 2048) or {+-}size{KMGTP}:
Last sector (2048-20971486, default = 20971486) or {+-}size{KMGTP}:
Current type is 8300 (Linux filesystem)
Hex code or GUID (L to show codes, Enter = 8300): 8e00
Changed type of partition to 'Linux LVM'

Command (? for help): p
Disk /dev/sdb: 20971520 sectors, 10.0 GiB
Model: Virtual disk
Sector size (logical/physical): 512/512 bytes
Disk identifier (GUID): 0A72FB8E-D076-480C-85D1-9BD670641A55
Partition table holds up to 128 entries
Main partition table begins at sector 2 and ends at sector 33
First usable sector is 34, last usable sector is 20971486
Partitions will be aligned on 2048-sector boundaries
Total free space is 2014 sectors (1007.0 KiB)

Number  Start (sector)    End (sector)  Size       Code  Name
1            2048        20971486   10.0 GiB    8E00  Linux LVM

Command (? for help): w

Final checks complete. About to write GPT data. THIS WILL OVERWRITE EXISTING
PARTITIONS!!

Do you want to proceed? (Y/N): y
OK; writing new GUID partition table (GPT) to /dev/sdb.
The operation has completed successfully.
```

5. Verify the newly created disk partition with **lsblk**.

```
li-admin@LogPoint:~$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                   8:0    0  100G  0 disk
├─sda1                8:1    0   30M  0 part
├─sda2                8:2    0   18G  0 part /
├─sda3                8:3    0  7.5G  0 part [SWAP]
└─sd                  8:4    0 74.6G  0 part
├─LogPoint--vg-app  253:0    0 18.6G  0 lvm  /opt
└─LogPoint--vg-data 253:1    0 55.9G  0 lvm  /opt/makalu/storage
sdb                   8:16   0   10G  0 disk
└─sdb1                8:17   0   10G  0 part
```

6. Create a new physical volume with the partition using **pvcreate /dev/sdb1**.

```
li-admin@logpoint:~$ pvcreate /dev/sdb1
Physical volume "/dev/sdb1" successfully created.
```

7. Extend the volume group first using **vgextend /dev/LogPoint-vg /dev/sdb1**. Running the **lsblk** command indicates that **LogPoint-vg** is the existing volume group and storage is the logical volume.

```
li-admin@logpoint:~$ vgextend /dev/LogPoint-vg /dev/sdb1
Volume group "LogPoint-vg" successfully extended
```

8. Extend the logical volume depending on your requirements.
   - For **opt**, extend the logical volume *opt* using **lvextend /dev/LogPoint-vg/app /dev/sdb1**.

```
li-admin@LogPoint:~$ lvextend /dev/LogPoint-vg/app /dev/sdb1
Size of logical volume LogPoint-vg/app changed from 18.62 GiB (4768 extents) to
28.62 GiB (7327 extents).
Logical volume LogPoint-vg/app successfully resized.
```

   - For **storage**, extend the logical volume *storage* using **lvextend /dev/LogPoint-vg/data /dev/sdb1**.

```
li-admin@LogPoint:~$ lvextend /dev/LogPoint-vg/data /dev/sdb1
Size of logical volume LogPoint-vg/data changed from 55.92 GiB (14316 extents) to
65.92 GiB (16875 extents).
Logical volume LogPoint-vg/data successfully resized.
```

9. Resize the logical volume.
   - For */opt*: **resize2fs /dev/LogPoint-vg/app**.

```
li-admin@LogPoint:~$ resize2fs /dev/LogPoint-vg/app
resize2fs 1.45.5 (07-Jan-2020)
Filesystem at /dev/LogPoint-vg/app is mounted on /opt; on-line resizing required
old_desc_blocks = 2, new_desc_blocks = 2
The filesystem on /dev/LogPoint-vg/app is now 7502848 (4k) blocks long.
```

   - For *storage*: **resize2fs /dev/LogPoint-vg/data**.

```
li-admin@LogPoint:~$ resize2fs /dev/LogPoint-vg/data
resize2fs 1.45.5 (07-Jan-2020)
Filesystem at /dev/LogPoint-vg/data is mounted on /opt/makalu/storage; on-line
resizing required
old_desc_blocks = 4, new_desc_blocks = 5
The filesystem on /dev/LogPoint-vg/data is now 17280000 (4k) blocks long.
```

10. Verify the increased disk size using **lsblk**.

```
li-admin@LogPoint:~$ lsblk
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
sda                   8:0    0  100G  0 disk
├─sda1                8:1    0   30M  0 part
├─sda2                8:2    0   18G  0 part /
├─sda3                8:3    0  7.5G  0 part [SWAP]
└─sda4                8:4    0 74.6G  0 part
├─LogPoint--vg-app  253:0    0 18.6G  0 lvm  /opt
└─LogPoint--vg-data 253:1    0 65.9G  0 lvm  /opt/makalu/storage
sdb                   8:16   0   10G  0 disk
└─sdb1                8:17   0   10G  0 part
└─LogPoint--vg-data 253:1    0 65.9G  0 lvm  /opt/makalu/storage
```

documentation@stormshield.eu