Scribbler Enterprise Linux – Installation and Maintenance Manual

The scribbler Linux version is released as a bundled package with optimized operating system. This document details the instructions on installing that on bare metal hardware or in virtual machine.

1 CONTENTS

2 Details 3
3 Obtain the Software Package 3
4 Prepare for the installation 3
4.1 For Bare Metal Hardware 3
4.2 For Virtual Machine 3
5 Operating System Installation 4
5.1 Booting the Installation Image 4
5.1.1 For BIOS based systems 4
5.1.2 For UEFI Based systems 5
5.2 Installation & Configuration 5
5.2.1 Wizard - Select your location 5
5.2.2 Wizard – Partition Disks 6
5.2.3 Partition Disks - New Install / Clean Install 6
5.2.4 Partition Disks - Upgrading an existing PC / Reusing existing partition 8
6 Application Installation 14
6.1 System Information 14
6.2 Scribbler Application Installation 15
7 Launch Application 16
8 OS Management 17
8.1 Changing IP Address 17
8.1.1 Change through command line 17
8.1.2 Change IP through OS Management Console 17
8.2 Configuring Additional Network Adapter 18

8.3 Changing Host Name 19
8.4 Changing NTP Configuration 20
8.5 Send the Base Linux OS Logging to Scribbler 21
8.6 Managing Disks 21
8.7 Recovery Console 22
8.8 Other useful commands 23
8.9 Joining to Active Directory Domain 23
8.10 Deploy Custom Root Certificate 24
8.11 Configuring Operating System SNMP Service 25
9 Application Upgrade 26
9.1 Full ISO 26
9.2 Scribbler OS update 26
9.2.1 Manual Way 26
9.2.2 Automated Way 27
9.3 Scribbler Application update 27
9.3.1 Manual Way 27
9.3.2 Automated Way 27

2 Details

The Scribbler OS is based on Debian Linux x64. As of this writing it is based on Debian 11.7 (x64). Make sure the latest version of this document is used.

3 Obtain the Software Package

The software package is distributed in the form of an iso image. Please contact the support / sales team for the download link.

4 Prepare for the Installation

Depending upon the target installation, different preparation methods are required.

4.1 For Bare Metal Hardware

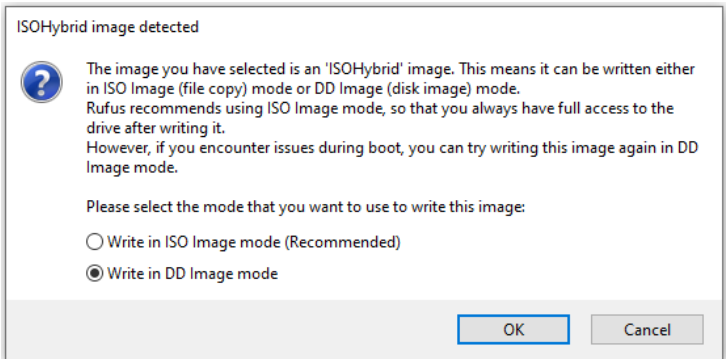
Burn the iso image into USB thumb drive / CD as a bootable installation media. Using SD card as a bootable installation media is not supported.

In Linux, the **dd** tool can be used to create bootable media.

- https://man7.org/linux/man-pages/man1/dd.1.html
- https://www.linuxandubuntu.com/home/how-to-burn-iso-image-to-dvd-and-usb-using-dd

On Windows, the rufus tool can be used to create bootable media.

- https://rufus.ie/en_US/
- Make sure to use "**dd image mode**" method while burning the image to USB thumb drive. "iso image mode" method is not supported.



4.2 For Virtual Machine

No special preparation is required. Mount the iso as installation cd and continue the hypervisor specific steps to start installation.

The guest tools for VMware, HyperV, KVM are already part of the iso.

5 Operating System Installation

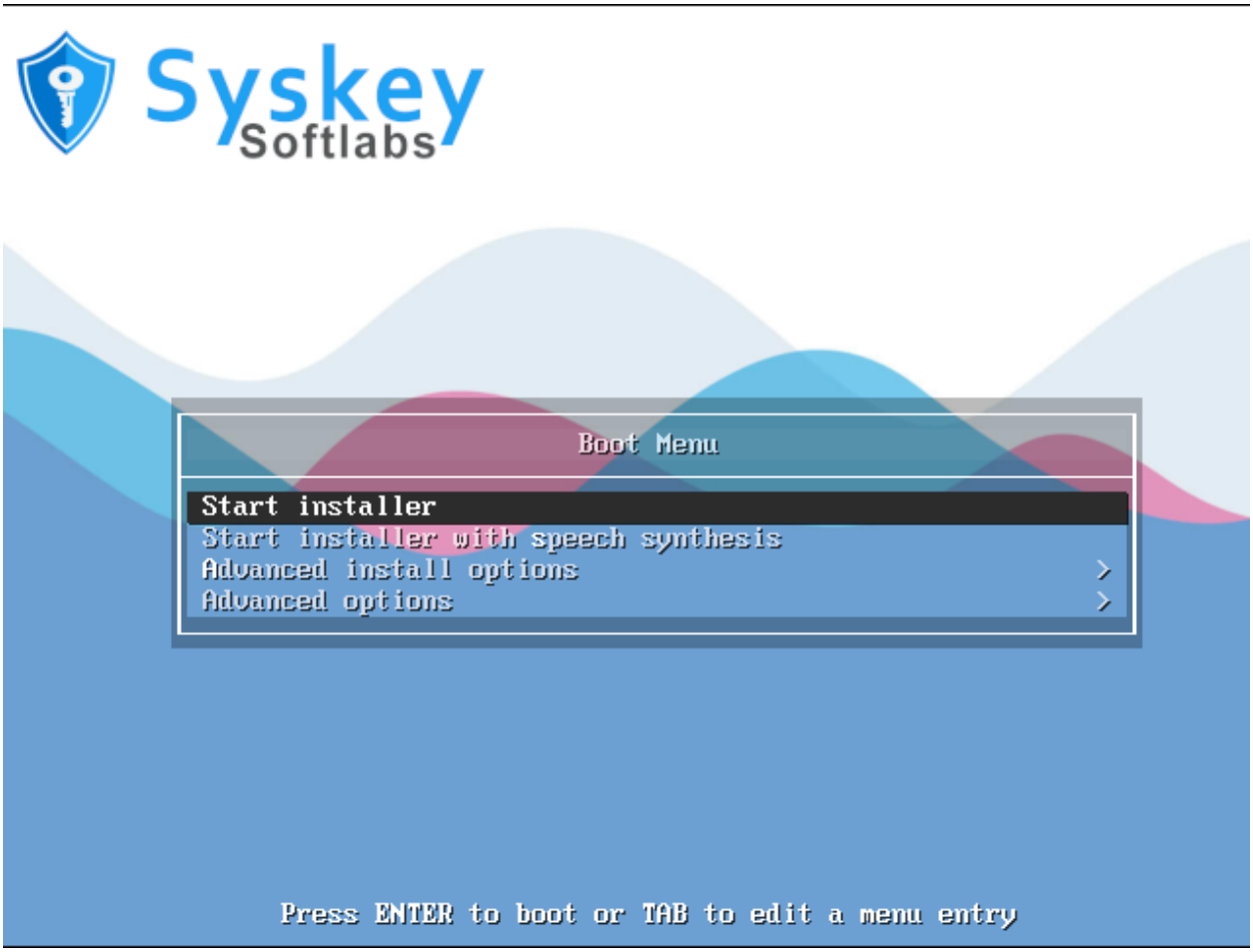
The first step of the installation process is installing the scribbler operating system.

5.1 Booting the Installation Image

- Insert the CD/USB [For bare metal hardware] or mount the iso [for virtual machine]
- And start the installation. The following boot loader will be shown.

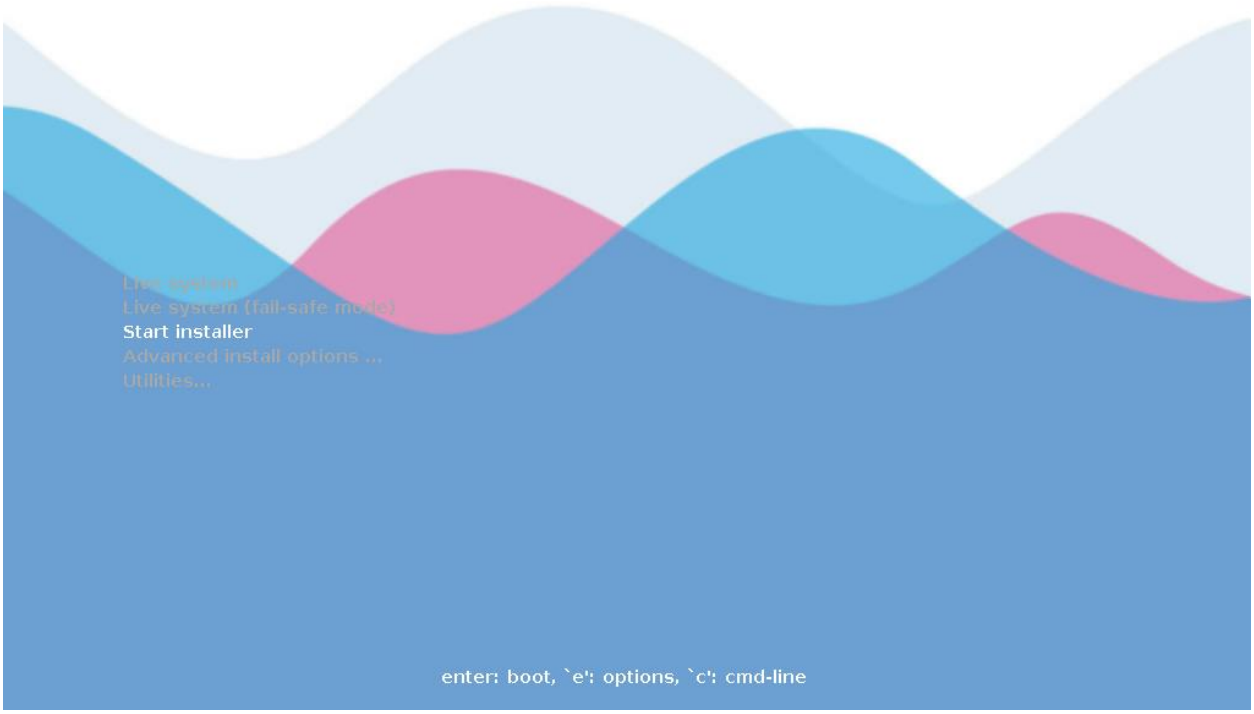
5.1.1 For BIOS based systems

- Select **Start Installer**



5.1.2 For UEFI Based systems

- Secure boot may work depending on the Linux key is loaded in the MOK.
- Select “Start Installer”



5.2 INSTALLATION & CONFIGURATION

The Graphical installer shows multiple wizards. Only the complex wizards are detailed here.

5.2.1 Wizard - Select your location

- Please choose the country. The relevant Time zone information will be asked later stage.
- The installer will load the files and start configuring other settings.

5.2.2 Wizard – Partition Disks

- This is an important step where the hard disk partitions are provisioned.
- The following partition scheme is recommended for scribbler installation
- The list may be bit different for UEFI based GPT.

S. No	Description	Mount point	Size	File System
0	EFI Boot Partition **Not required for BIOS based systems**		512 MB	FAT 32
1	Linux Root	/	20 G	ext4
2	Swap area / Virtual Memory	Not Applicable	Half of RAM	Not Applicable
3	To store scribbler log data	/data	**Min 20 GB**	ext4
4	To store log backup. For storing on the same disk, it can be a folder under data partition **[Default]**	Not Applicable	Not Applicable	Not appliable
	To store backup in additional disk, Separate partition is recommended.	/backup	As Required	Ext4

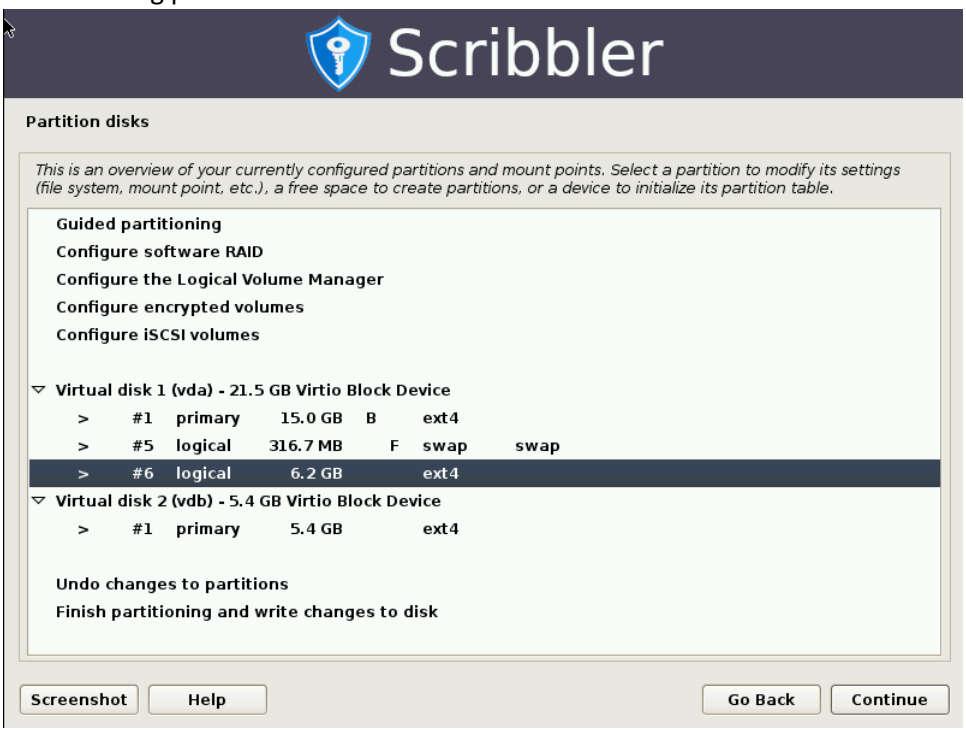
- The /data partition is not mandatory but **recommended**. Scribbler installer at later stage can be configured to use /data. This will be handy when doing major OS version upgrades.
- Additional disk for backup is not required in case you want to use network backups.
- If the computer has more than one disk, automatic partitioning will not happen, and manual partitioning is required.

5.2.3 Partition Disks - New Install / Clean Install

Please follow the below instructions for new install or clean install (wipe out everything and start a fresh)

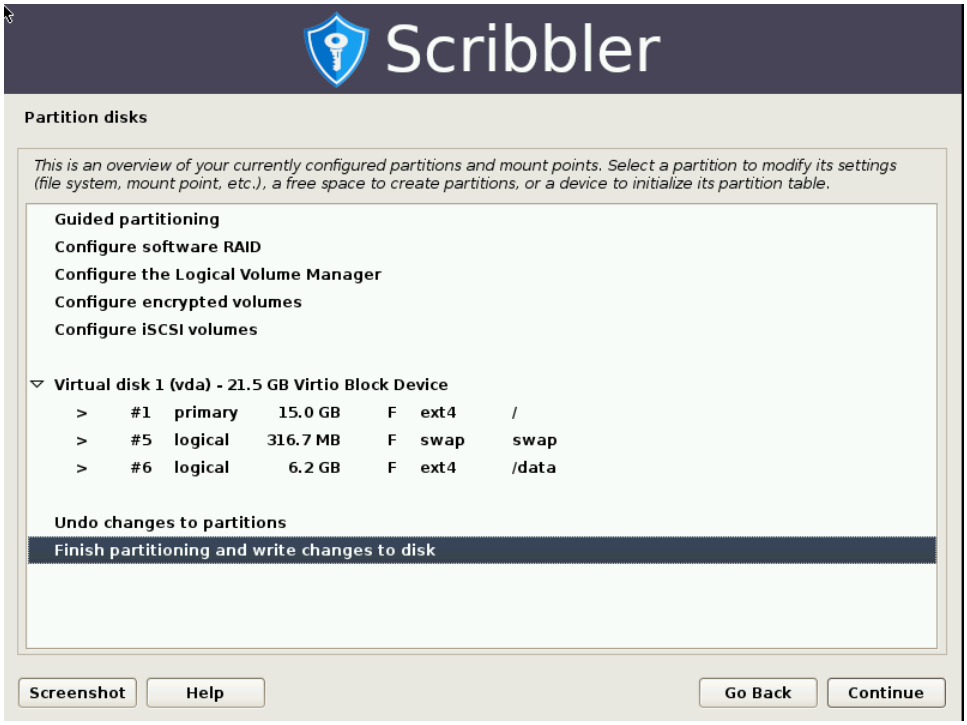
- Varity of partitioning types (manual, guided, LVM, encryption) are supported. Please follow-on screen instructions to perform the required partitioning scheme.
- Below screens is an example for standard manual partitioning for BIOS based systems.
- For EFI based systems an EFI system partition (bootable) is additionally required.

- Delete all the existing partitions



  - Select the partition to be deleted and double click / click continue.
  - Select **“Delete the partition”** and double click.
  - And repeat the steps until you delete all the partitions.

- Create new partitions as detailed in the reference table. Finally, it should be something like this.

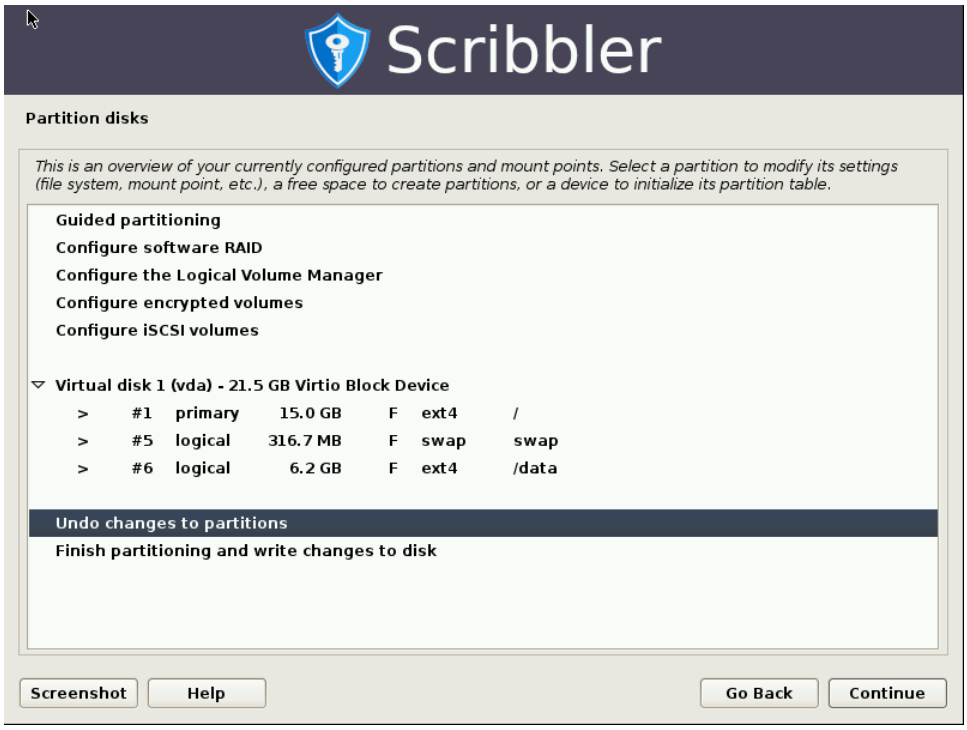


  - The backup partition can be created or configured after installation as well. But the root, swap and data are required for the installation.

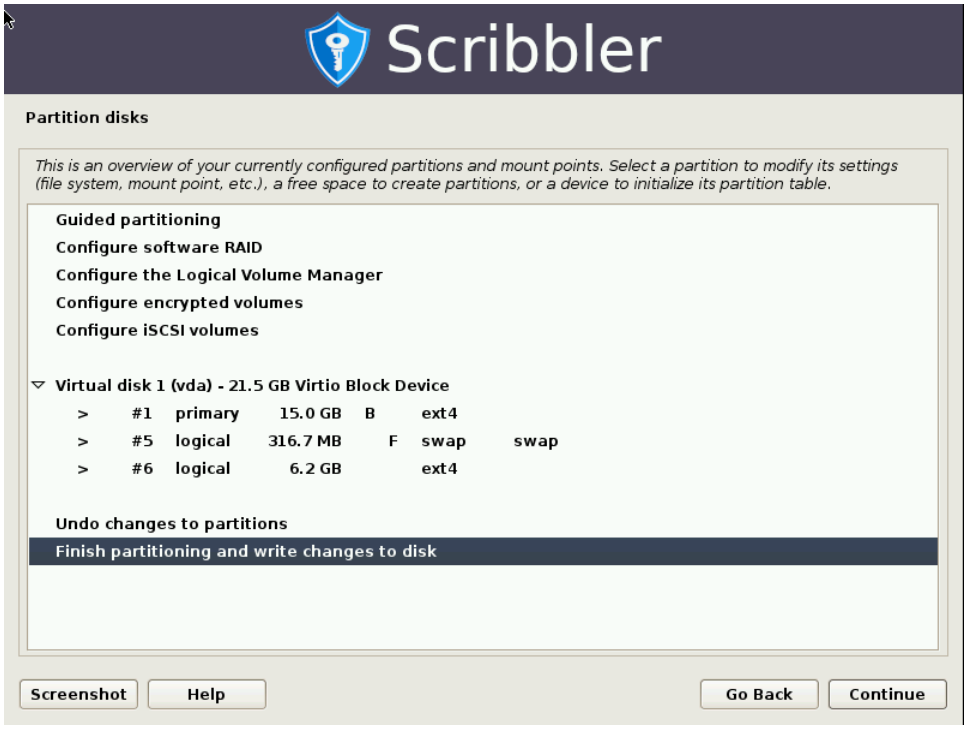
5.2.4 Partition Disks - Upgrading an existing PC / Reusing existing partition

For the upgrade, it is better to keep the existing data partition and format the rest (instead of deleting rest of the partition)

- Take a backup of the data partition [Not required but always recommended]
  a. While system is running,
    i. Uninstall the application [Important. Without this backup is not reliable]
      1. Login to the SSH console of the computer.
      2. Navigate to the folder "/opt/scribbler-installer/"
      3. Run "sudo ./uninstall-scribbler.ps1"
      4. Wait for it to complete.
    ii. Copy all the contents of the /data folder into some network drive or other backup medium.
  b. After system shutdown,
    i. Boot from another live CD/USB stick and identify the data partition and copy the data to a network drive or to USB drive.
- For Single Disk systems
  a. The installer will always propose a new partition table regardless of existing installation was there or not.
  b. Discard the partition proposed by installer by double clicking the "Undo changes to the partitions".



c. That will undo the partition table and display the existing partition table as shown below.

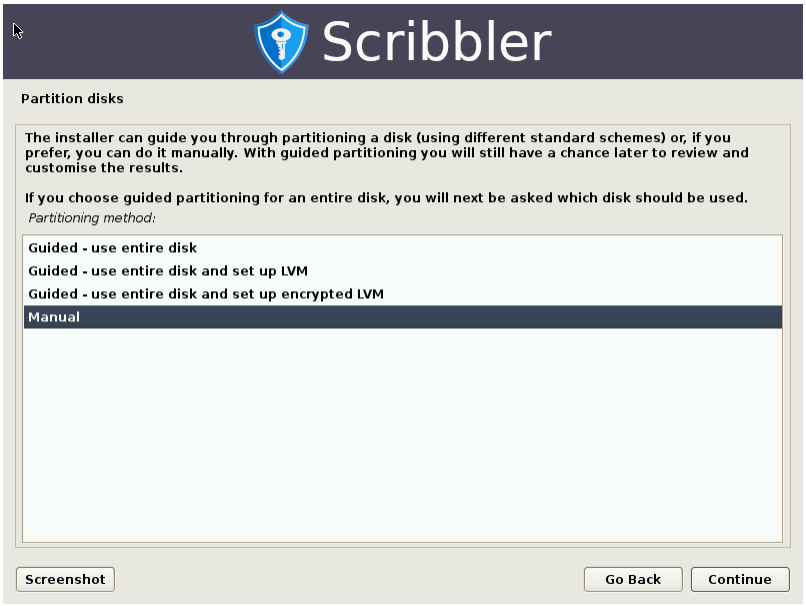


d. In the above sample scribbler is already installed on the PC and is showing the existing partitions

   i. Disk 1 #1 – root partition
   ii. Disk 1 #5 – swap
   iii. Disk 1 #6 – data partition

e. The partition labels (/data, /,) will not be shown on this screen. That must be known beforehand based on the previous installation.
f. Skip the next section “Multi Disk systems”.

- For multi disk systems, start the manual partition.

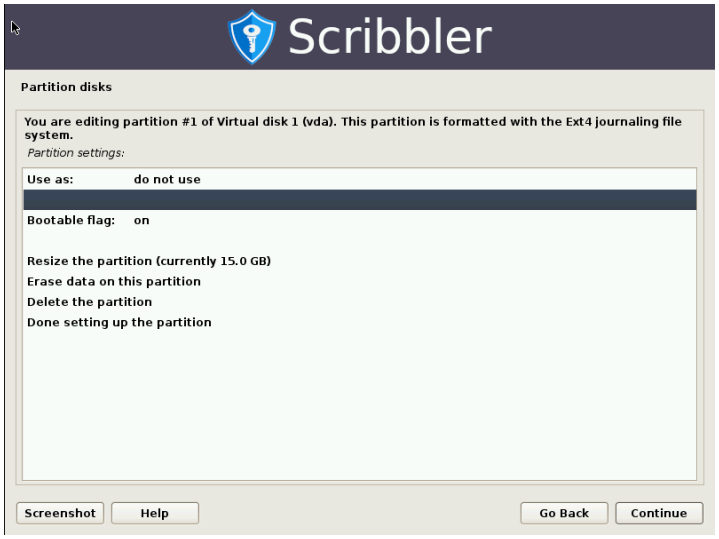


a. The existing partitions will be shown like this.

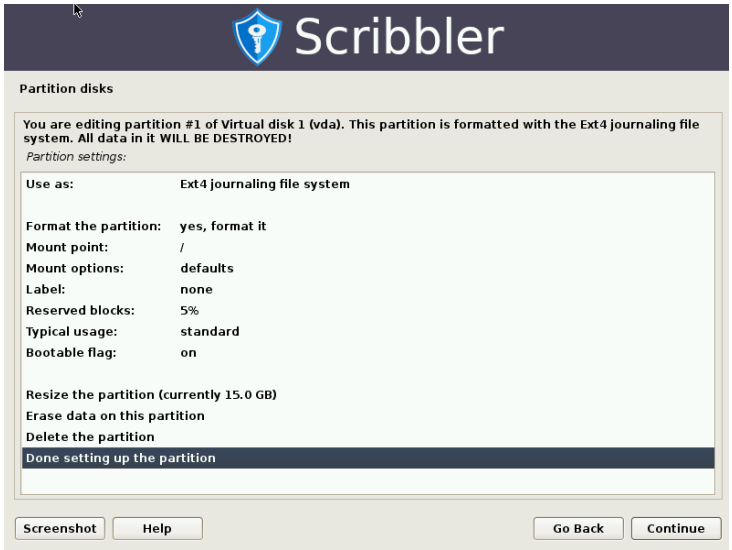
b. In the above sample, scribbler is already installed on the PC and is showing the existing partitions
    i. Disk 1 #1 – root partition
    ii. Disk 1 #5 – swap
    iii. Disk 1 #6 – data partition
    iv. Disk 2 #1 – partition for backup

c. The partition labels (/data, /, /backup) will not be shown on this screen. That must be known beforehand based on the previous installation.

- Configure Existing Partitions
  a. All the disk labels referred in the following texts are based on the screen shot shown in step 1a. Actual labels may vary please be careful when doing this step.
  b. Root Partition - Format and reuse
     i. Double click the “disk 1 - #1”. The disk details will be like this. Without filesystem info and mount point

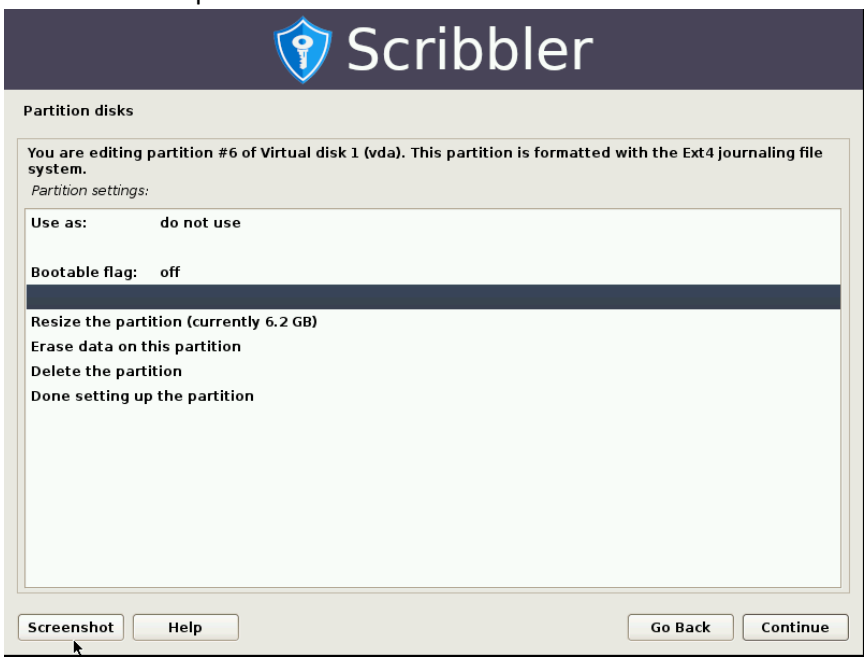


     ii. Update “Use as” to “Ext4 Journaling file system”
     iii. Update “Format the partition” to “yes, format it”
     iv. Update “Mount Point” to “/”
     v. Finally, it should look like below.



     vi. Double click the “Done setting up the partition”
  c. Swap Partition – No change required keep as it is.
  d. Data Partition – Do not Format just assign mount point.

i. Double click “disk 1 - #6”. The disk details will be like this. Without filesystem info and mount point

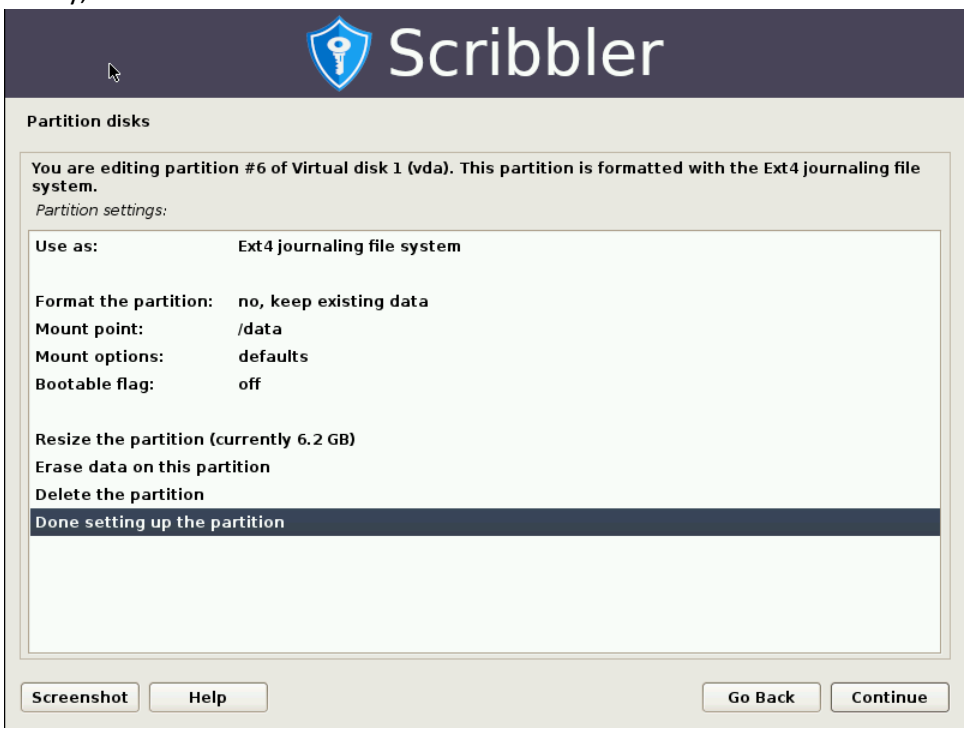


ii. Update “Use as” to “Ext4 Journaling file system”

iii. Update **“Format the partition” to “no, keep existing data”**

iv. Update “Mount Point” to “/data” (Enter manually option is required for custom mount point)

v. Finally, It should be like this

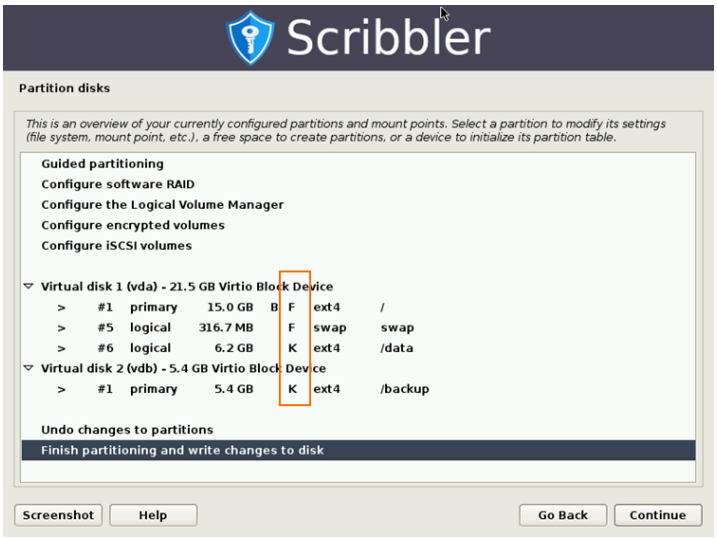


vi. Double click the “Done setting up the partition”

e. (Only if used previously) Backup Partition - Do not format just assign.

i. Repeat the steps like the data partition but use a different mount point e.g., “/backup” It should match with the previous mount point.
ii. If a different mount point is provided, then after installation scribbler configuration must be changed to point this new mount point.

f. Finally, the partition disks will look like the following.

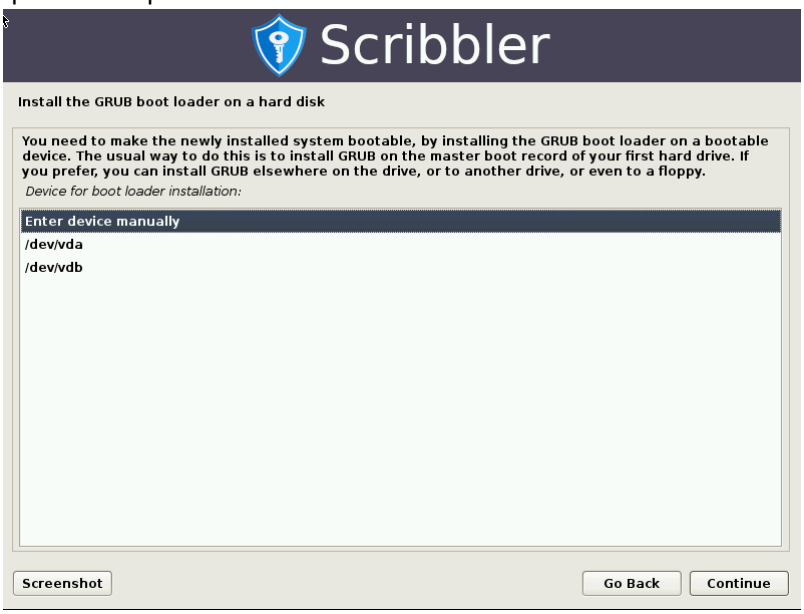


g. F -> Format partition, K -> Keep partition, B -> Boot.
h. Click “Finish partitioning and write changes to disk” and click continue.

- Partitioning is completed.

5.2.4.1 *Wizard – Install GRUB bootloader on a hard disk*

- Select the device on where to install the boot loader and continue. It is typically the disk where the root partition is placed.



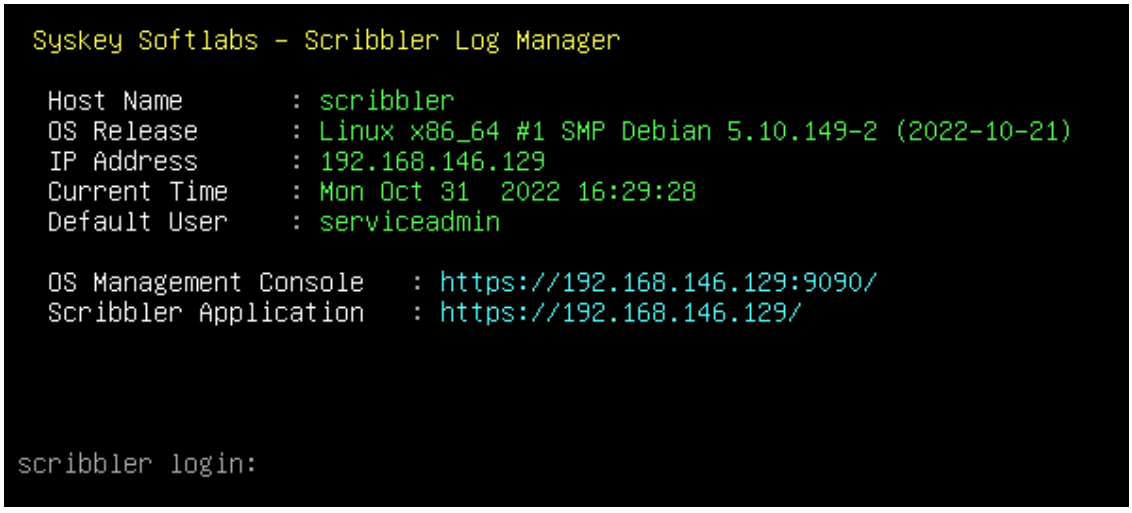
- That is the end of the operating system installation.
- System will reboot. Make sure you remove the USB / CD ROM so that the system will boot from the hard disk. If not, please change the boot order in the BIOS

6 APPLICATION INSTALLATION

After the OS installation please restart the computer and login.

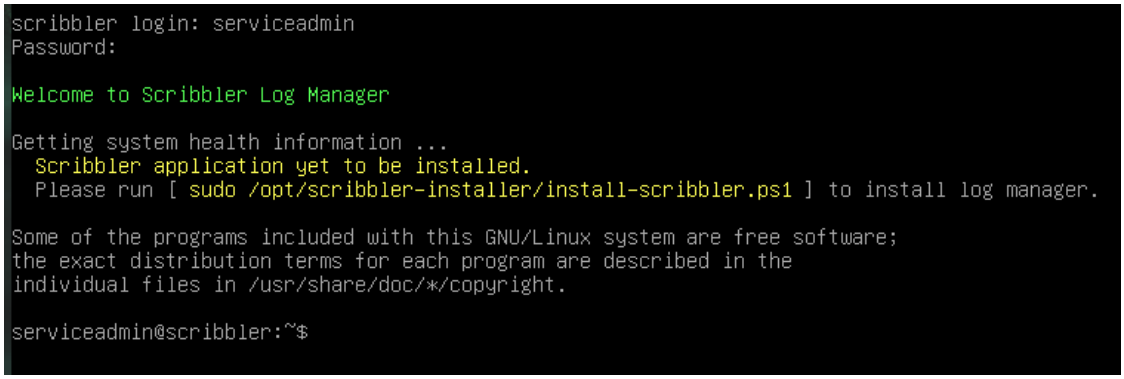
6.1 SYSTEM INFORMATION

- Upon successful boot, The user will be greeted by the welcome screen
    a. General information about the system will be shown including the IP address.



- Log with the user **serviceadmin** and password **scri@@ler7**
    a. Upon successful logon, The following screen will be shown which contains instructions to install the scribbler application.

b.

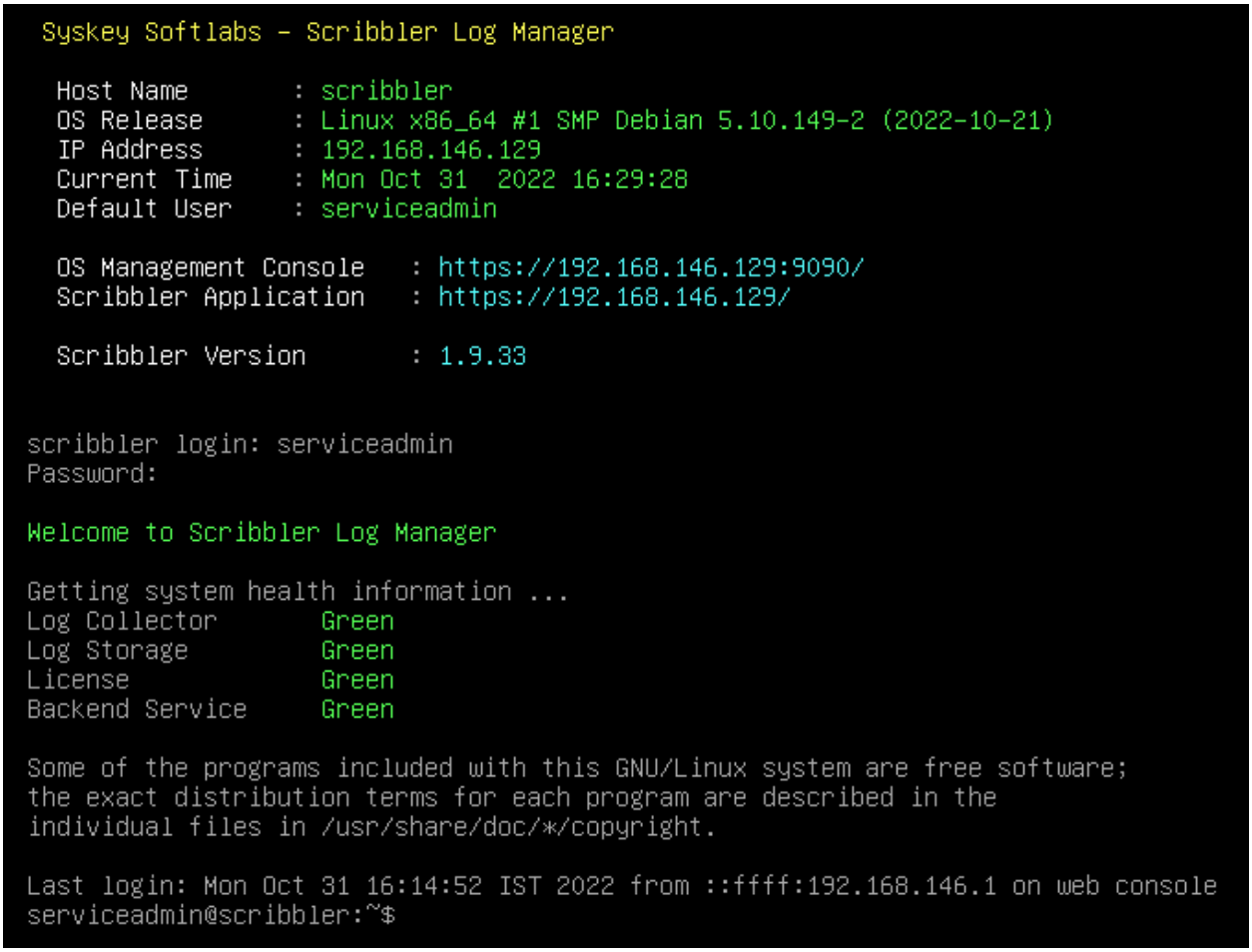


- **[Important]** Change the password and keep it safe after successful login.
    a. Change Password command: *passwd*
- By default, DHCP is enabled, and the system will receive an IP from DHCP server. If there is no DHCP server present in the network, A static IP can be configured Refer section Changing IP Address

6.2 Scribbler Application Installation

Install the scribbler application by running the following command [which is displayed on the screen]

- *sudo /opt/scribbler-installer/install-scribbler.ps1*
- Please provide the password of the serviceadmin user to continue sudo prompt.
- The installation will start and asks for the location for the data disk.
- Please read the onscreen instructions carefully
- Please provide "/data" (the partition created earlier). Or any other location which has sufficient space.
- The installation will take almost 3-10 mins.
- Once the installation is completed, wait for 5 mins, and restart the computer.
- After installation, on every successful login, The system will show the health information of various modules as shown below.



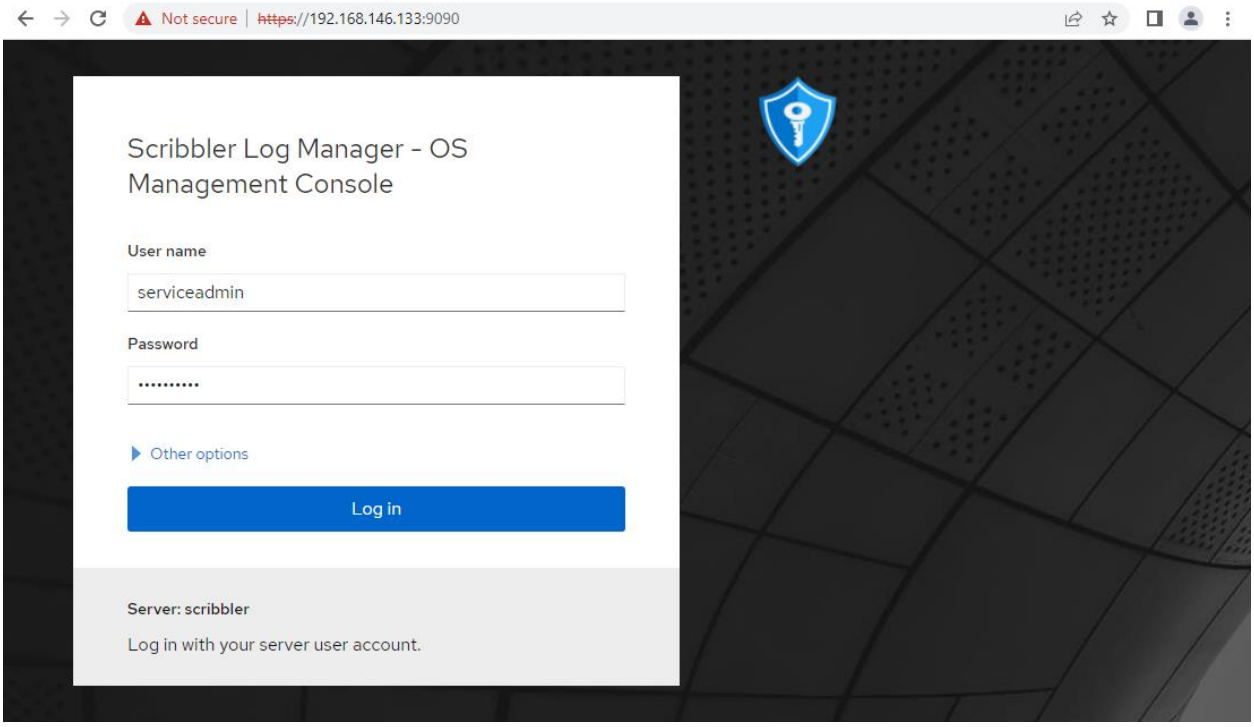
7 LAUNCH APPLICATION

- Open a web browser from a connected PC and browse the URL shown in the server terminal console. It usually the following
    a. https://<serverip>
    b. The application by default deployed with self-signed certificates. So please ignore the warning.
- Credentials for Scribbler Application:
    a. User: **Admin**
    b. Pass: **Admin**
- Scribbler application loads and the user will be greeted with the application dashboard.
- **[Important]** Change the username or password or both after the login as per organization security policy.

8 OS MANAGEMENT

To manage operating system level configuration (configure NTP, format disk,) a separate web-based management console is provided.

The management console is running on port 9090. https://<ipaddress>:9090/ . The management console is running secured by https self-signed certificate. The browser warning can be ignored.



The credentials are the same as the operating system login (SSH) credentials.

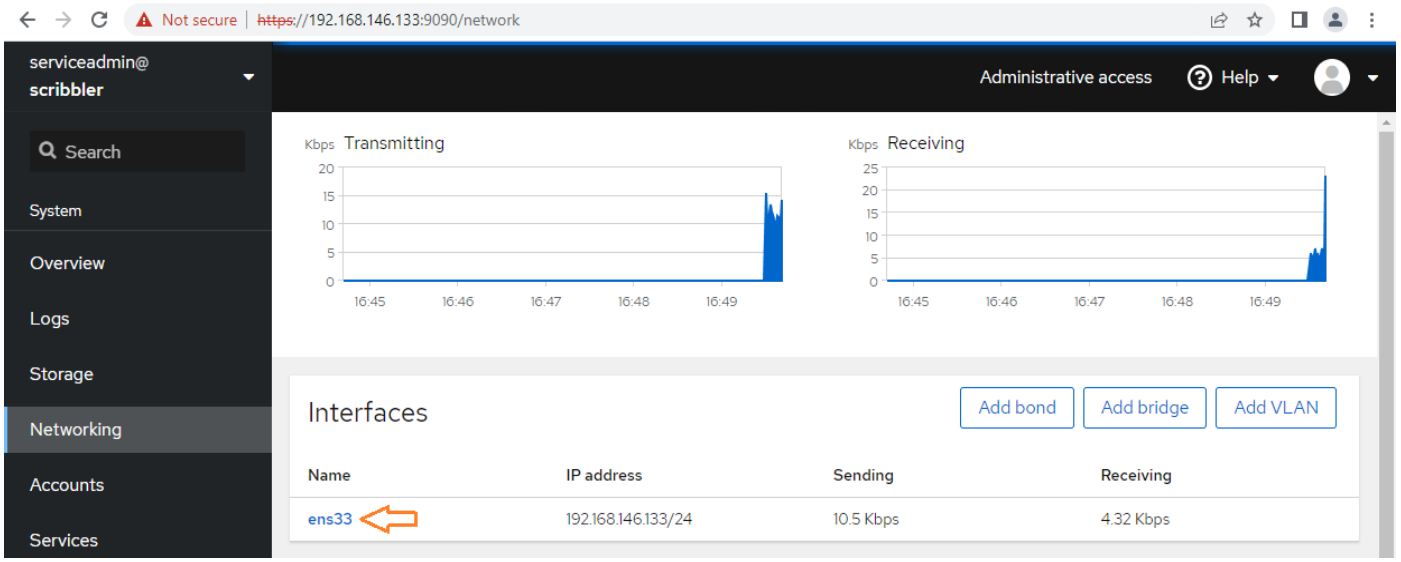
8.1 CHANGING IP ADDRESS

8.1.1 Change through command line

- Login to the console with service admin user.
- Run **nmtui** command and follow the on-screen instructions.
    - `serviceadmin@scribbler:~$ nmtui`

8.1.2 Change IP through OS Management Console

- Login to the web OS management console
- Go to System -> Networking. And click on the interface name.



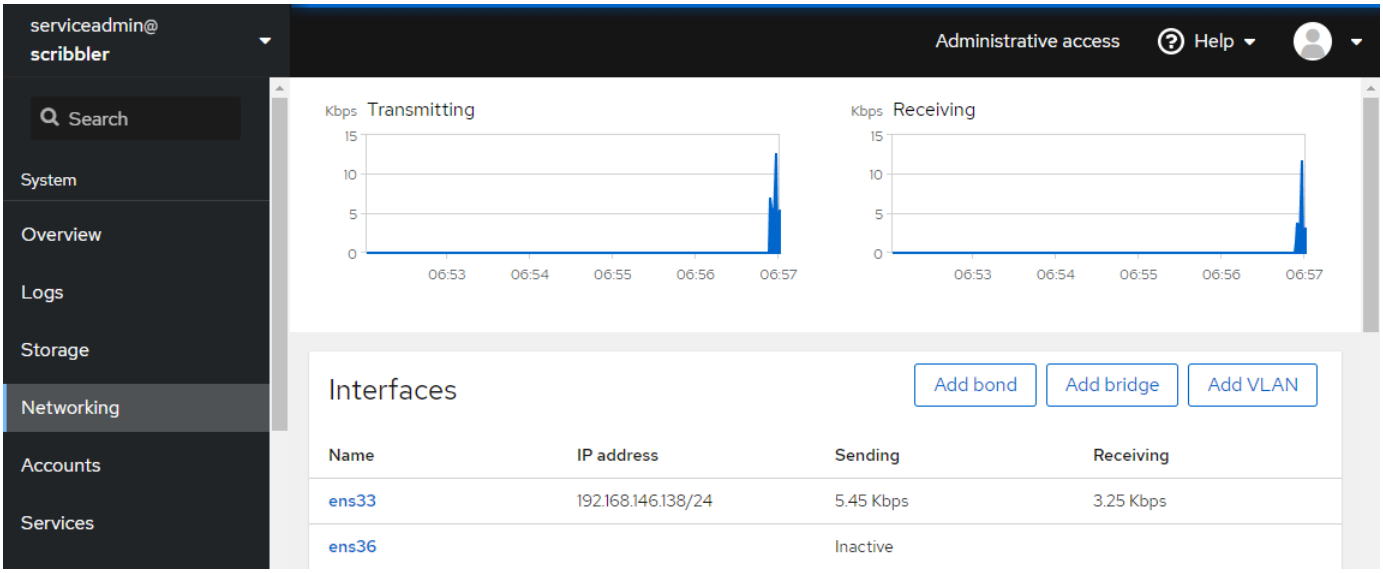
- *Note : If the network interface appears under unmanaged interfaces section, then most probably the /etc/network/interfaces may be manually edited. Please revert that change and try with **nmtui** or OS management console.

8.2 Configuring Additional Network Adapter

Newly added network adapters automatically configured if there is DHCP server available. Otherwise, the IP address must be manually configured as described in step 8.1.2

In some rare scenarios, if the adapter is not configurable through management interface the following will be helpful.

Please go into the Networking tab as shown below



- Take note of the inactive adapter name. In the above screen shot it is “**ens36**”.
- Go to Tools -> Terminal. That will open the terminal window and run the following command
- `sudo nmcli c add type ethernet ifname <interfacename> con-name <new profile name>`
    - interface name -> is the name shown in the nmcli / web management console networking section.
    - profile name -> Any name . Make sure it is not clashing with existing names like "Wired Connection 1"
- **`e.g.,`** `sudo nmcli c add type ethernet ifname ens36 con-name Wired2`

8.3 CHANGING HOST NAME

The Linux system requires the correct hostname to be present in both /etc/hosts and /etc/hostname files. It works with different names in those files, but random slowness or failures are expected.

- To update the hostname to “scribbler-demo-new”.
- Edit the /etc/hosts (use nano /etc/hosts)
    - Put the right hostname with FQDN. Below is an excerpt of a localhost and valid hostname configuration

```
127.0.1.1 scribbler-demo-new.local scribbler-demo-new
127.0.0.1 localhost.localdomain localhost
```

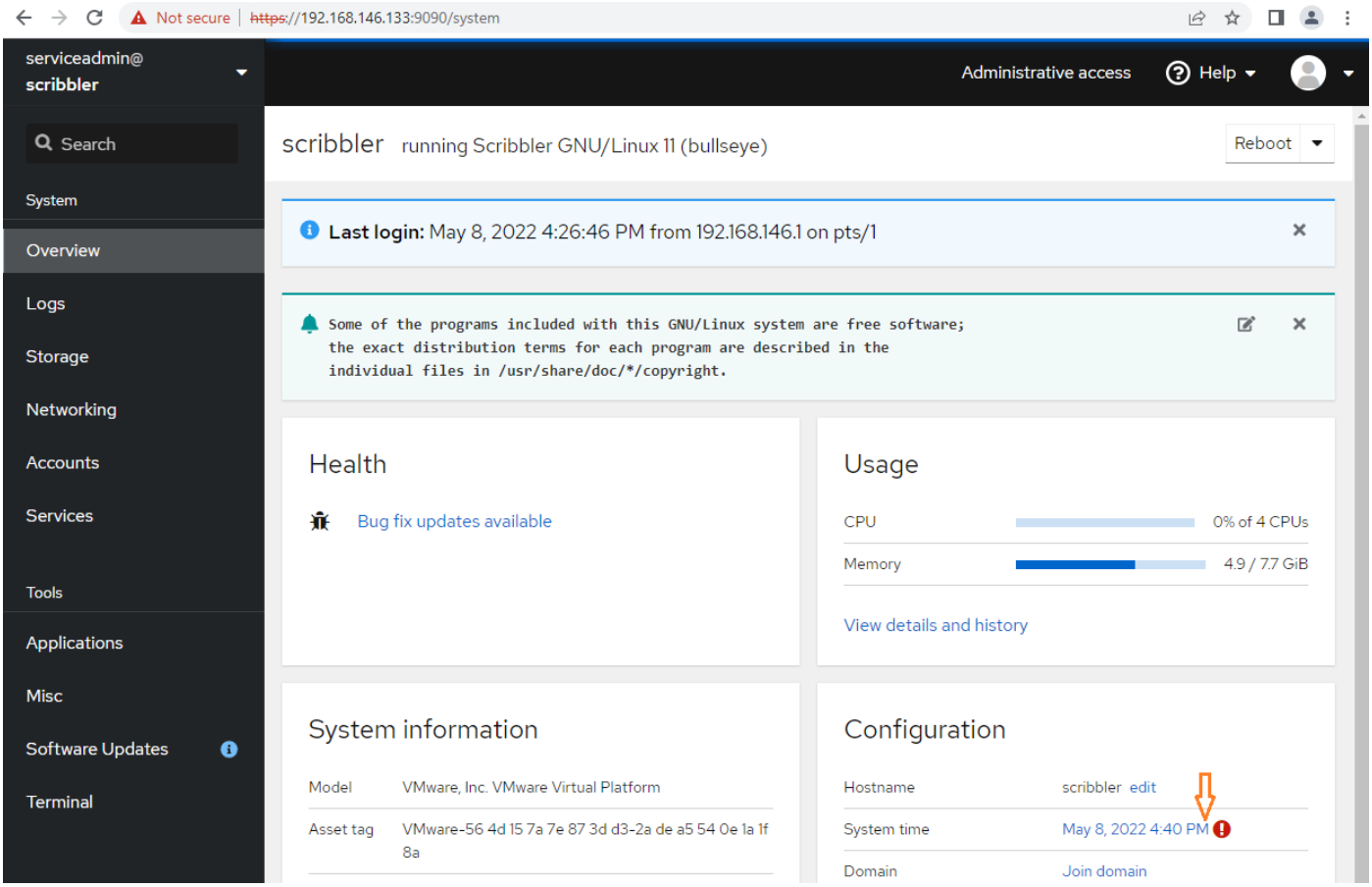
- Edit /etc/hostname (use nano /etc/hostname)

```
scribbler-demo-new
```

- Reboot the pc.

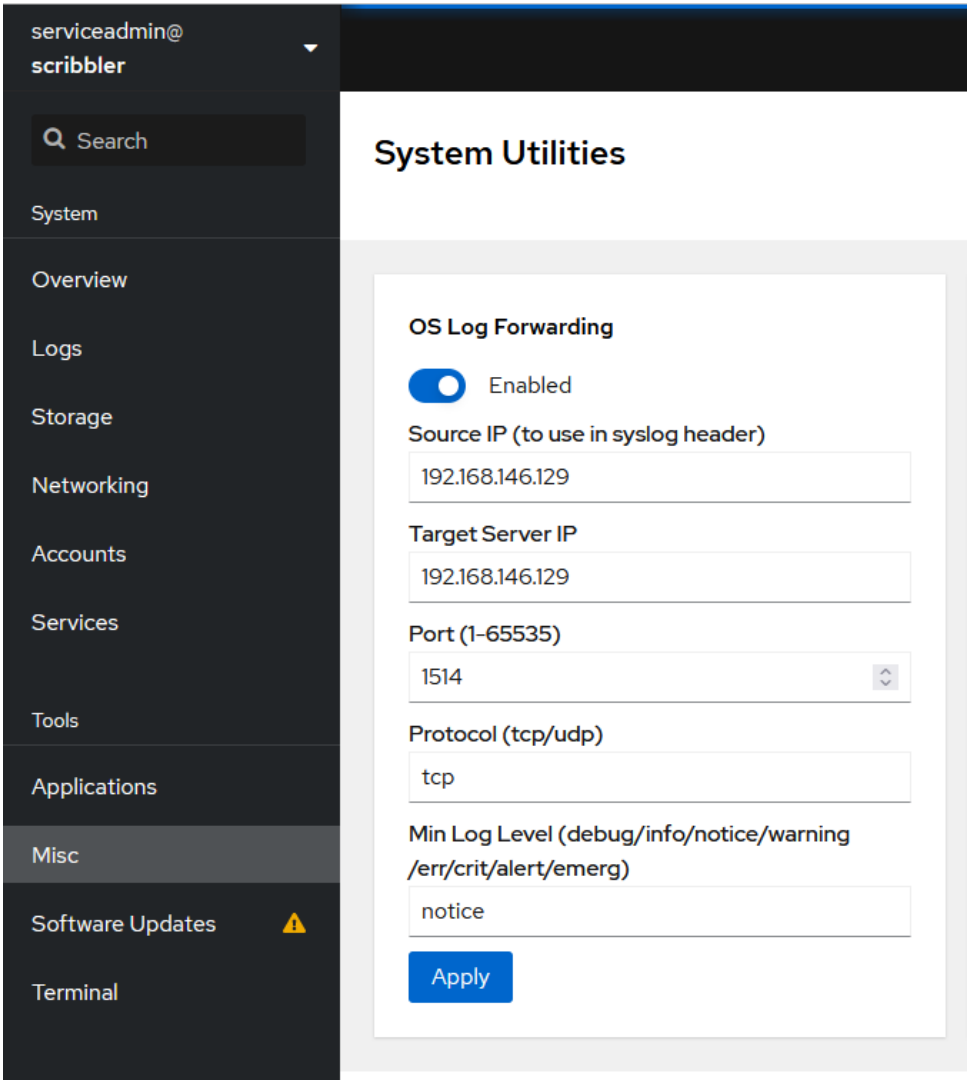
8.4 CHANGING NTP CONFIGURATION

- Login to the web management console
- Go to System -> Overview (as shown below) and click on the date.
- Follow the on-screen instructions to update the NTP time



8.5 Send the Base Linux OS Logging to Scribbler

- The base operating system logs can be configured to send to scribbler application.
- Please open the *Misc -> System Utilities -> OS Log Forwarding* section.
- Please provide the correct details.
- notice will be the good level.
- [Important]: The char casing is important for all log levels.



8.6 Managing Disks

- Login to the web management console https://<ip-address>:9090/
- Navigate to System -> Storage.
- And follow onscreen instructions to partition the disks.
- **Note:** Make sure the following custom options are provided while mounting removable media. Otherwise After the system shutdown and drive removed, The system will not boot.
    - `defaults,nofail,x-systemd.device-timeout=30s`
    - The above will indicate the device is not required for booting.

- **Note 2**: If a custom disk is planned to be used for scribbler backup. Make sure to set the correct permissions as listed below.
    - Assuming /backup is the mounted folder.
    - Open the terminal inside web management console and run the following commands.
    - `sudo chgrp -Rf scribbler /backup`
    - `sudo chown -Rf scribbler /backup`
    - `sudo chmod g+s /backup`
    - `sudo chmod -Rf g+rw /backup`

8.7 Recovery Console

On rare scenarios (disk corruption, etc.) the system may not boot properly. Since the root account is locked due to security reasons the system will not allow access to the recovery console as well.

In those cases, Modify the bootloader entries and set the init to directly load the shell.

- When the boot screen is active. Type letter '**e**'

- That will show boot menu the edit screen

- As underlined above, At the end of the Linux entry, add following
    - "`init=/bin/bash`" and press F10 key.
- That will boot the system, but the root file system will be mounted as ro (readonly).
- Run the following command to mount it to rw (read write) and make changes.
    - `mount -o rw,remount /`
- Once done, remount to readonly and shutdown using shutdown button on the device.
    - `mount -o ro,remount /`

8.8 OTHER USEFUL COMMANDS

Scribbler OS and Application creates some handy command aliases for easier management.

- status -> Get the status of all the application modules.
- **sudo /opt/syskey/scribbler/start-scribbler.ps1** -> Starts all scribbler modules.
- **sudo /opt/syskey/scribbler/stop-scribbler.ps1** -> Stops all scribbler modules.

8.9 JOINING TO ACTIVE DIRECTORY DOMAIN

Scribbler OS supports joining to active directory. The steps to configure is same as Debian Linux 11.

Note: All the following instructions assume the domain is "syskey.local". Change it according to the requirement.

- Prerequisites
  - Update Scribbler OS to 11.6.3
    - To Check Run the following command
      - `cat /etc/scribbler/os-release-manifest.json`
    - Output scribbler version if the file missing it is on lower version.
    - If the OS is on older version, Upgrade to 11.6.3 . Refer Section Scribbler OS update
    - Check the current DNS is pointing to AD DNS
      - Run `cat /etc/resolv.conf`
  - Set the DNS of the Scribbler OS to point to AD DNS server.
    - Login to OS Management Console [https://<scribbler OS IP>:9090]
    - Navigate to Networking and edit the interface by clicking the interface name
    - Click **edit** on IPv4 settings
    - Disable automatic DNS (if enabled)
    - Add the DNS IP and click Apply
    - Ensure it is applied by running `cat /etc/resolv.conf`
- Join to AD
  - Using the OS Management Console
    - Login to OS management Console https://<ip>:9090
    - Go to Overview -> Configuration
    - Click **Join Domain** and follow on-screen instructions
      - Hint: The Computer OU can be left blank.
  - Using commands
    - sudo realm join -U <UserName> <Domain>
    - The username should be a user in the domain who has domain admin privilege.
      - *e.g.:* `sudo realm join -U Administrator syskey.local`
- Add required groups to whitelist for logging into Linux OS
  - Space in group names should be surrounded by double quotes.
  - `sudo realm deny --all`
  - `sudo realm permit -g syskeyadmins@syskey.local`
  - `sudo realm permit -g syskeynonadmins@syskey.local`
  - `sudo realm permit -g "Domain Admins@syskey.local"`

- Tweak The AD Configurations
  - Edit "/etc/sssd/sssd.conf"
    - `sudo nano /etc/sssd/sssd.conf`
  - Ensure the following values exist under [domain/syskey.local]. If not add / update.
    - `cache_credentials = False`
    - `entry_cache_timeout = 60`

- Setup Automatic home directory creation for domain users upon login
  - Edit /etc/pam.d/common-session
    - `sudo nano /etc/pam.d/common-session`
  - Add the following line [**Single line**]
    - `session optional pam_mkhomedir.so skel=/etc/skel umask=077`

- Making a domain group as Linux admins
  - Caution: Incorrectly editing this file may result in security vulnerabilities.
  - Create/Edit file named ad-admins under /etc/sudoers.d
    - `sudo visudo /etc/sudoers.d/ad-admins`
  - Add a separate line for each AD group which requires sudo privilege in Linux.
    - The following code will make all users of "Domain Admin" group will get sudo (admin) permissions on Linux
    - The percentage character is mandatory.
    - Any space in group name should be escaped by a backward slash.
    - `%Domain\ Admins@syskey.local ALL=(ALL) ALL`

- Restart the sssd service
  - `sudo systemctl restart sssd`

- Validating AD Integration
  - Login using SSH with AD user
    - `ssh -l administrator@syskey.local 192.168.146.131`
  - Login to OS Management Console with AD user

Once configured with the above instructions the AD users can login to the scribbler Linux operating system.

8.10 Deploy Custom Root Certificate

There are cases where deploying a custom CA certificate to the Scribbler Linux operating system may be required. Follow the below instructions to deploy certificate.

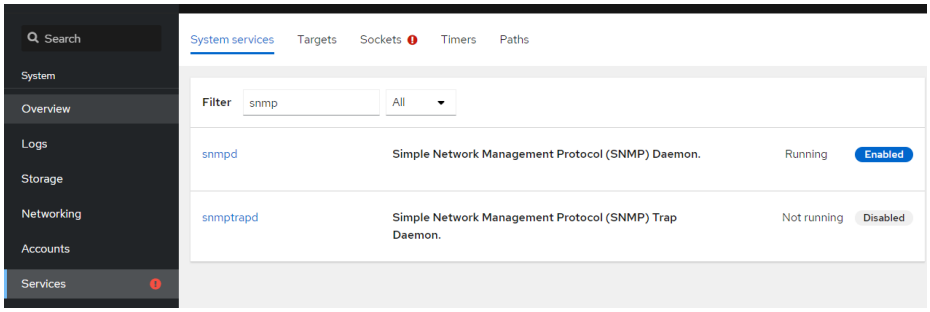
- Get base64 encoded public key certificate in a file
- Make sure the file is in .crt extension.
- Copy the file to the Scribbler Linux machine. And run the following commands.
- `sudo cp domain-ca.crt /usr/local/share/ca-certificates/domain-ca.crt`
- `sudo update-ca-certificates`

8.11 Configuring Operating System SNMP Service

This section details configuring the SNMP services of the Linux operating system. To configure Scribbler Log Manager's own agent, Please refer Scribbler Log Manager application manual.

By default, SNMP service is enabled and configured to run on 127.0.0.1. It can be disabled in the Services sections of the OS management console.

Important: It is strongly advised to configure the SNMP service in read only mode. i.e., All the write operations should be blocked through proper access controls.

- Prerequisites
  - Update Scribbler OS to 11.6.4
- Make sure the snmpd service is enabled.
  - 

- Modify the configuration add the IP address & password.
  - `sudo nano /etc/snmp/snmpd.conf`
  - Set IP Address to listen as a comma separated at the end of **agentaddress** section.
    - `agentaddress  127.0.0.1,[::1],192.168.153.138`
  - Update the password aka community string for v1 and v2. Change it from public to something else on these lines.
    - `rocommunity public default -V systemonly`
    - `rocommunity6 public default -V systemonly`
- Restart the service.
  - `sudo systemctl restart snmpd`
- That's all

The default configuration exposes only minimal data over SNMP. If the entire tree needs to be exposed configure the required views. Please refer the Debian OS snmpd manual.

For more advanced configuration (enable v3 and v3 users) please refer the Debian SNMP manual.
https://manpages.debian.org/unstable/snmpd/snmpd.conf.5.en.html

9 APPLICATION UPGRADE

This section details the application upgrades. New versions of the applications are released in three forms

9.1 FULL ISO

Contains the scribbler operating system iso with latest application.

- This is **not preferred** for upgrades due to its complexity.
- This can also be used to upgrade existing systems by formatting the root partition and reinstall. The /data and /backup partitions **should not be formatted** otherwise the data will be lost.
- OS Installation: Follow the instructions on the [Partition Disks - Upgrading an existing PC / Reusing existing partition] to install the operating system without formatting /data.
- App Installation: Follow the instructions in Scribbler Application Installation
    - During the installation, Please provide the existing data partition when asked.

9.2 SCRIBBLER OS UPDATE

9.2.1 Manual Way

Contains only operating system security patches and updates. The OS updates come in two forms. One for UEFI installations and another for BIOS based installations. The package name contains UEFI/BIOS to indicate the update package type.

Pick the right update package for the installation and copy that to that computer and run the package.

- Copy the **scribbler-os-update-package_*.gpg.tar** to the scribbler server using any one of the following options
    - Login to OS management console and use the **Files** option [Available only from 11.6 OS version]
    - Copy it to a USB thumb drive and mount it on the scribbler computer.
    - Network Transfer through SCP
        - `scp <source> <destination>`
        - e.g: ***scp ./syskeyot-os-update-package_11.5.11.gpg.tar serviceadmin@ip_address:/home/serviceadmin/***
    - FileZilla software can also be used to transfer files.
- Upgrade
    - SSH to the server with `serviceadmin` user.
    - Stop the scribbler application
        - Run `**sudo /opt/syskey/scribbler/stop-scribbler.ps1**`
    - Upgrade
        - ***sudo /opt/systemtools/install-os-update-package.ps1 ./syskeyot-os-update-package_11.5.11.gpg.tar***
    - **Note:** To upgrade to OS versions 11.6.3 / 11.6.4 the above command must be run twice.
    - The scribbler OS will be updated to latest patches.

- Reboot the computer.

9.2.2 Automated Way

Through the SyskeyOT Central Cockpit solution, the updates can be pushed from a central console to all the instances of scribbler.

9.3 SCRIBBLER APPLICATION UPDATE

9.3.1 Manual Way

- Copy the application update package [***scribbler*_date_version.*tar***] to the log manager server using any of the steps mentioned in 9.2
- Uninstall existing scribbler application
  - Login to the ssh console. Run the following command.
  - ***sudo /opt/scribbler-installer/uninstall-scribbler.ps1***
- Extract the copied scribbler application update package
  - ***tar -xf scribbler_2022-11-01_1.9.36.tar --one-top-level***
  - That will create a folder named "***scribbler_2022-11-01_1.9.36***"
- Install the new version
  - cd ***scribbler_2022-11-01_1.9.36***
  - ***sudo ./install-scribbler.ps1***
  - The installation process will start and provide the same data folder previously used. It should be "/data" unless a different folder is used previously.
  - Make sure you are providing the same data folder which is used previously. Otherwise, scribbler is unable to use the previous datastore/database.

9.3.2 Automated Way

Through the SyskeyOT Central Cockpit solution, the updates can be pushed from a central console to all the instances of scribbler.