FortiSIEM 3500F – Migration Guide

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

08/24/2020
FortiSIEM 5.3.3 3500F Migration Guide

TABLE OF CONTENTS

FSM 3500F Migration **4**
Step 1: Upgrade FSM 3500F to v5.0.1 4
Step 2: SSH to FortiSIEM instance 4
Step 3: Stop all back-end processes 4
Step 4: Bring the Database server up 4
Step 5: Backup CMDB 4
Step 6: Copy the /data directory to a remote location 5
Step 7: Re-image the appliance 5
Step 8: Restore CMDB 7
Step 9: Update the Disk name in the Database 8
Step 10: Configure the Network 8
Step 11: Apply License 8
Step 12: Reset SVN password 8
Step 13: Delete Worker cache file 8

FSM 3500F Migration

Starting Release v5.0.0, FortiSIEM 3500F will run on bare metal, bypassing the OpenStack Hypervisor layer. This simplifies the installation, maintenance and improve performance. It is recommended to migrate the current data on your appliance and move to the new FSM 3500F OS - basically run on bare metal but retain the old data.

Follow the steps in this document for migration:

Step 1: Upgrade FSM 3500F to v5.0.1

- Follow the instructions in the 'Upgrading FortiSIEM' section of 3500F - Hardware Configuration Guide here to upgrade to FortiSIEM v5.0.1.

Step 2: SSH to FortiSIEM instance

- After upgrading FSM 3500F to v5.0.1, SSH to FortiSIEM host as:
  `ssh -i /opt/devstack/ao-fsm.key root@169.254.254.2`

Step 3: Stop all back-end processes

1. Run the commands in the following order:
   a. `phtools --stop all`
   b. `service crond stop`
   c. `/opt/phoenix/phscripts/bin/phxctl stop`
2. Run `phstatus` and make sure all processes are down.

The processes - `phMonitor` and `Node.js` maybe be up and can be ignored.

Step 4: Bring the Database server up

1. Run `service postgresql-9.1 start`.
2. Run `phstatus` to make sure the `DBSrv` process is up.

Step 5: Backup CMDB

1. Run the archive script to create an archive version of the CMDB using the command:
   `/opt/phoenix/deployment/db_archiver.sh`

The archived file will be saved at `/data/archive/cmdb/<phoenixdb_Date_Time>`

2. Run `du -sh /data` to check the disk size in the remote system and make sure that there is enough space to copy the database.

Step 6: Copy the /data directory to a remote location

1. Run `rsync -avzh /data/ root@<remote-IP>:/backups/`
   Make sure that the trailing `/` is used in the final two arguments in the `rsync` command.
2. Make sure the `/data` files are copied to the remote location.

Step 7: Re-image the appliance

Ensure that the following prerequisites are met before re-imaging FortiSIEM.

Hardware	Software
Peripherals • USB Keyboard • USB Mouse • VGA Monitor **USB Thumbdrive** • 4 GB Thumbdrive (for Linux installation) • 8 GB Thumbdrive (for FortiSIEM appliance image)	• Ubuntu Desktop Setup Files • Rufus (Bootable USB Utility) • FortiSIEM Appliance Image

a) Create Bootable Linux image

1. Connect 4GB USB drive to the system (desktop or laptop).
2. Open Rufus.
3. Select the following settings for the USB:
   a. **Partition scheme and target system type**: MBR partition scheme for BIOS or UEFI
   b. **File system**: FAT32
   c. **Cluster size**: 4096 bytes (default)
   d. **Quick Format**: Enable
   e. **Create a bootable disk using**: ISO image
4. Click on the 'CD-ROM' icon and select the Ubuntu Setup ISO.
5. Click **Start** and allow Rufus to complete.
   Once finished, the disk is ready to boot.
   Note: Alternatively, you can use the Ubuntu guide for creating a USB drive with Ubuntu.

b) Copy FortiSIEM image to USB

1. Connect 8 GB USB Drive to the system (desktop or laptop).
2. Open **Windows Explorer** > right-click **Drive** > click **Format**.
3. Select the following options:
   a. **File system**: NTFS
   b. **Allocation unit size**: 4096 bytes
   c. **Quick Format**: Enable
4. Copy the image file to USB drive.
   For example: `FSM_Full_Super-Worker_RAW_HW_VA-5.3.3.1677.zip`
5. Safely remove the USB drive from the desktop or laptop by unmounting it through the Operating System.

c) Uninstall an existing FortiSIEM version

1. Connect to the console/SSH of the FortiSIEM appliance.
2. Run the following command:
   `sudo execute fsm-clean`
3. Allow the above command to run and power-off the FortiSIEM appliance.
4. Power on the FortiSIEM appliance and connect to the console/SSH of the FortiSIEM Host.
5. Delete an existing Volume group by running:
   `sudo vgremove cinder-volumes-lvmdriver-1`
6. Identify the 63TB disk name by running:
   `sudo fdisk -l | less`
   Note: This drive will be referred as `/dev/sda` in the following steps.
7. Wipe the file system of the 63TB disk by running the following commands:
   - `sudo wipefs --all /dev/sda2`
   - `sudo wipefs --all /dev/sda1`
   - `sudo wipefs --all /dev/sda`

d) Configure 3500F BIOS to boot into USB Drive

1. Connect the 4 GB USB drive to the FortiSIEM appliance.
2. Reboot the FortiSIEM appliance.
3. During the boot screen, press **F11** to login to the boot options.
4. Select the option to enter into the BIOS set up.
5. Select the option for Boot options.
6. Select the 'USB drive'.
7. Save the options and quit set up.

e) Re-image 3500F boot drive from USB Linux

1. Power on the FortiSIEM appliance.
2. Once the FortiSIEM appliance loads from the USB drive, click **Try Ubuntu**.
   a. Connect the 8 GB USB drive to the FortiSIEM appliance.
   b. Open a terminal.
   c. Type the following command to identify the FortiSIEM boot disk (29.5GiB):
   `sudo fdisk -l`.
   Note: This drive will be referred as `/dev/sdb` in the following steps.
3. Enter into `root` while in the terminal using the command:
   `sudo -s`
4. Determine the mount point of this drive using the command:
   `df -l`
   Note: For this guide, the assumption for the 8 GB mount point is: `/media/ubuntu/123456789/*`
5. Copy the image from the 8 GB disk to the FortiSIEM boot disk.
6. Extract the zipped raw image and copy the image into SATA disk (32GB). For example, use the command:
   `unzip -c FSM_Full_Super-Worker_RAW_HW_VA-5.3.3.1677.zip | dd of=/dev/sdb status=progress`
7. Once this is completed, power off the FortiSIEM appliance using the command:
   `shutdown -h now`
8. After shutdown, remove both USB drives from the FortiSIEM appliance.
9. Power on the FortiSIEM appliance.
10. Login as 'root' user with password 'ProspectHills'.
11. Run the command: `execute format disk`
12. Run the command: `execute factoryreset`
13. Run `/opt/vmware/share/vami/vami_config_net` script to install FortiSIEM.
    The system will reboot after the script is complete.

Do not apply the License yet.

Step 8: Restore CMDB

1. Run the commands to stop the back-end processes:
   a. `service crond stop`
   b. `/opt/phoenix/phscripts/bin/phxctl stop`
   c. `phstatus` - make sure all `ph* processes` except `phMonitor` is down.
2. Copy the directory `/data` back from the remote location using the rsync tool:
   `rsync -avzh root@<remote-IP>:/backups/ /data/`
3. Bring the Database server up using the command:
   `service postgresql-9.1 start`

4. Run `phstatus` to make sure `DBSrv` is up.
5. Restore the Database using the command:
   `/opt/phoenix/deployment/db_restore.sh /data/archive/cmdb/<phoenixdb_Date_Time>`
   (From Step #5)

Step 9: Update the Disk name in the Database

- Run `psql -U phoenix -d phoenixdb -c "update ph_sys_conf set value='/dev/mapper/FSIEM3500F-phx_data' where property='disk_name';"` to update the disk name in the Database.

Step 10: Configure the Network

- Run `/opt/vmware/share/vami/vami_config_net` to configure the network. The system will reboot after the script is complete.

Step 11: Apply License

- Use the existing 4.10.0 license.

Step 12: Reset SVN password

- Run `/opt/phoenix/deployment/jumpbox/phsetsvnpwd.sh` (admin/admin*1/super).

Step 13: Delete Worker cache file

- Run `rm /data/cache/worker_mon_job.xml`.

Migration is now complete. Make sure all the devices, user-defined rules, reports, dashboards are migrated successfully.