NetGuardians

NG|Screener Installation

Ljupce Nikolov

May 2019, Yverdon-les-Bains

Summary

- System Requirement
- Virtual Machine Creation
- NG|OS Installation
- Components Installation
- Connectors Installation
- Checking Install

System Requirements

Local / Test Install

- What will be used during training
- **Min 6 GB RAM**
- Turn ON Virtualization hardware extensions
  - Intel VT-x / AMD-V

Usual Install

- What will be required on production servers
- Min 8 GB RAM
- Min 4 CPUs
- Fast Hard drives (Ideally SSDs)

NetGuardians

Virtual Machine Creation

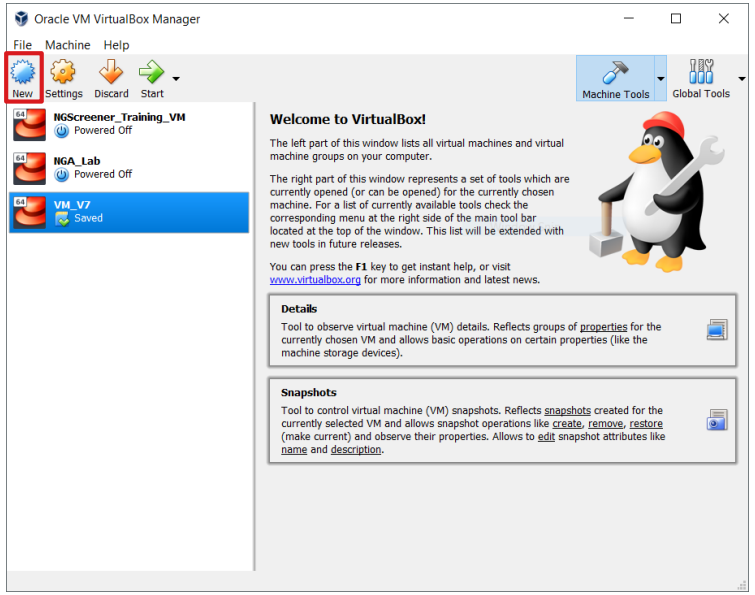
swiss made software

Virtual Machine Creation

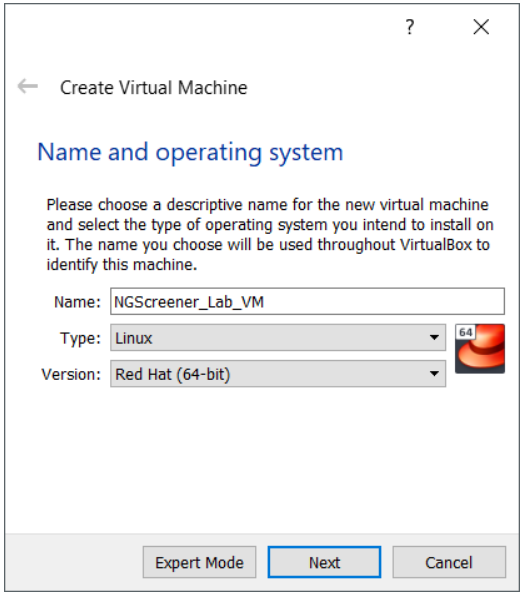
- Virtual Box
  - Version 5.2.8 Minimum
- Used for testing purpose on local machine
- Will be needed during labs

Virtual Machine Creation

Step 1: Create a new VM

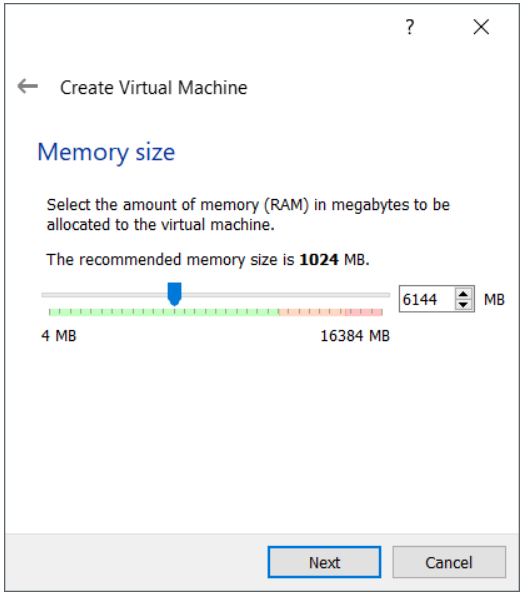


Step 2: Select OS (RedHat 64 bits)

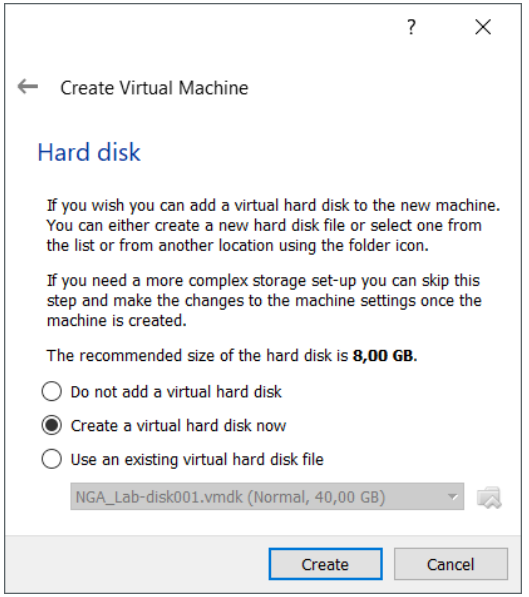


Virtual Machine Creation

Step 3: Set RAM size (6 GB min)

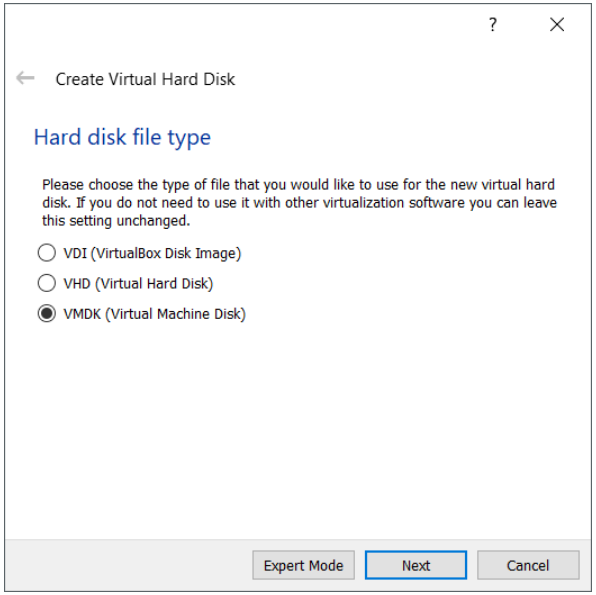


Step 4: Create 1st Hard disk

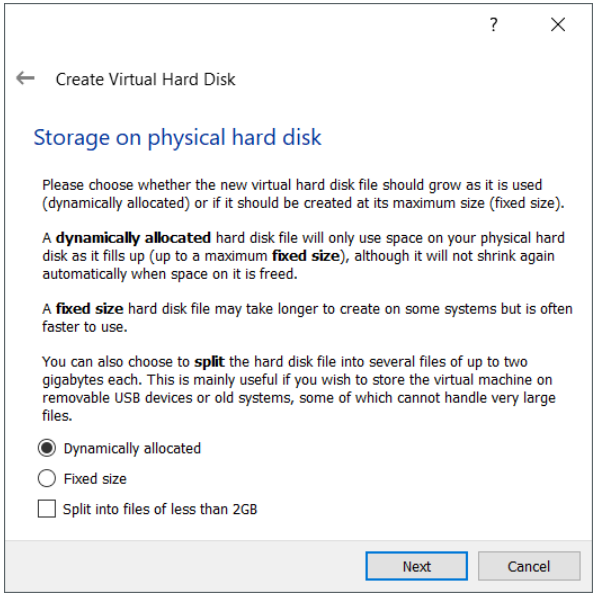


Virtual Machine Creation

Step 5: Type of disks to VMDK

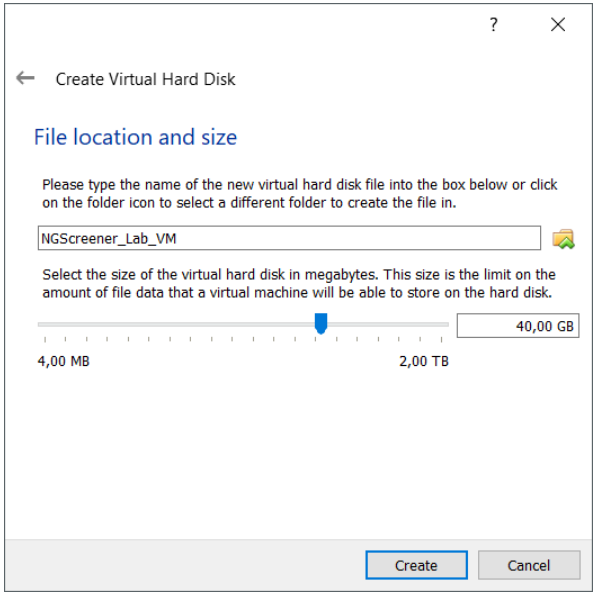


Step 6: Set to Dynamically allocated

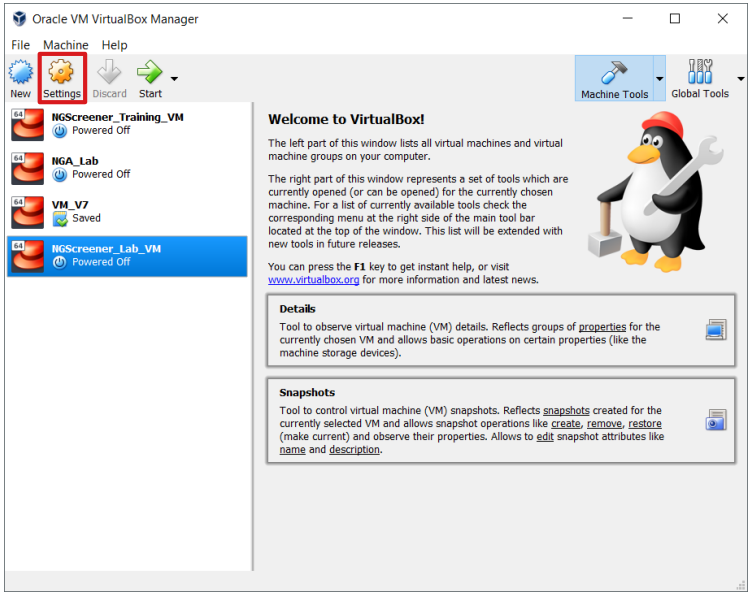


Virtual Machine Creation

Step 7: Set Size (min 40 GB)

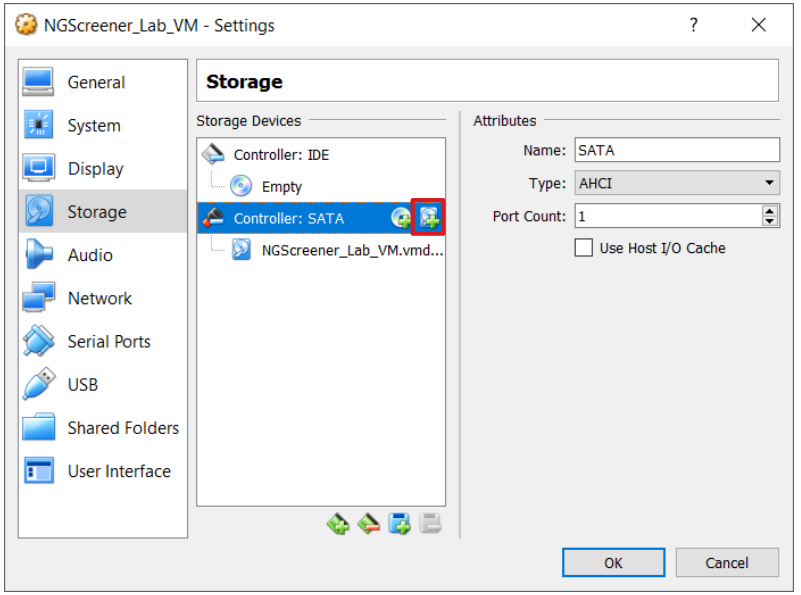


Step 8: VM is created. Go to setting to tune it

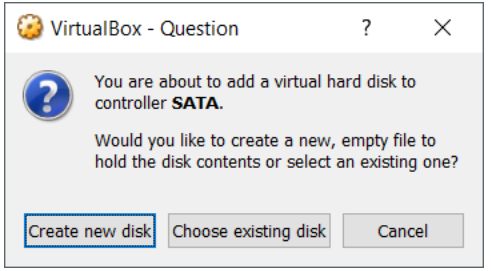


Virtual Machine Creation

Step 9: Create 2 additional disks

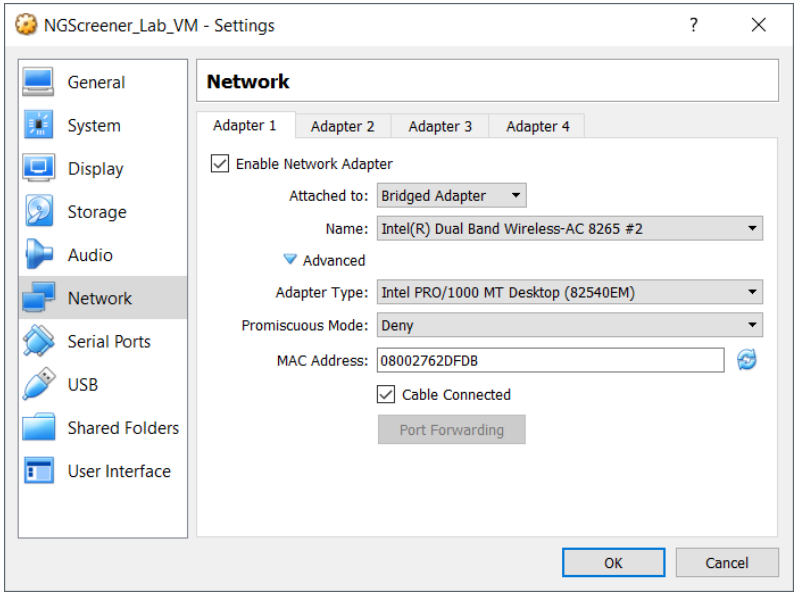


Step 10: Create New disks (cf. steps 4-7) 50/60 GB

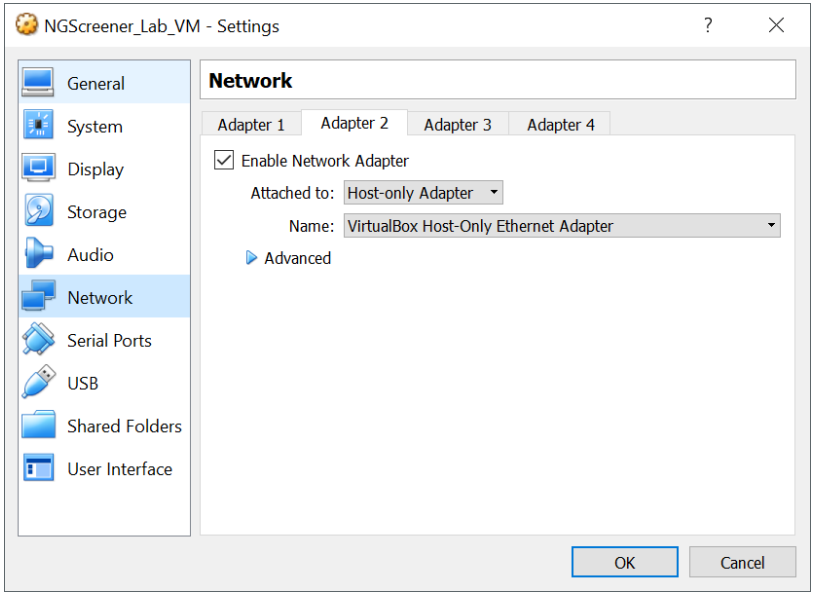


Virtual Machine Creation

Step 11: Set network to Bridged Adapter

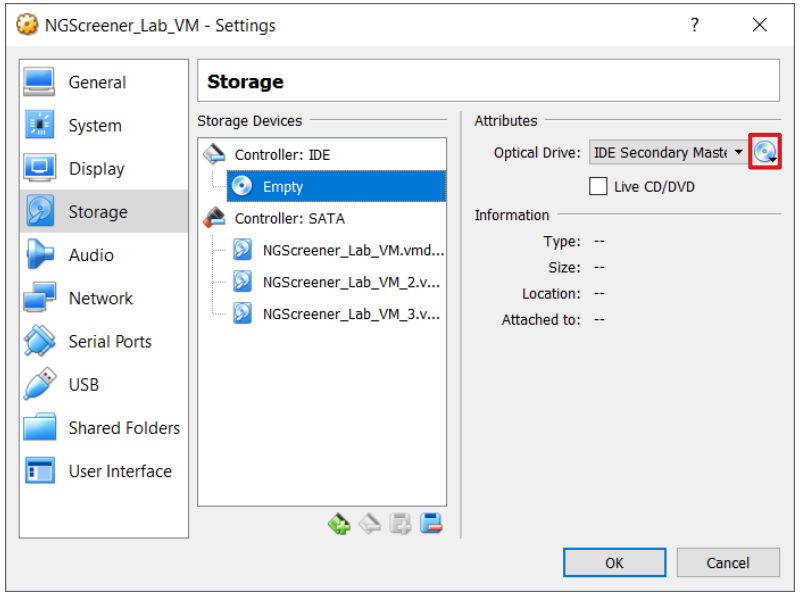


Step 12: Add a 2nd adapter as Host-only Adapter



Virtual Machine Creation

Step 13: Mount NG|OS iso file



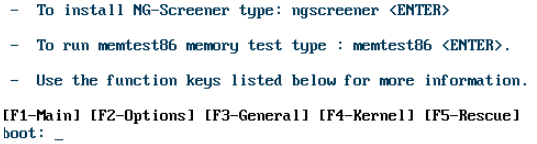
NetGuardians

NG|OS Installation

swiss made software

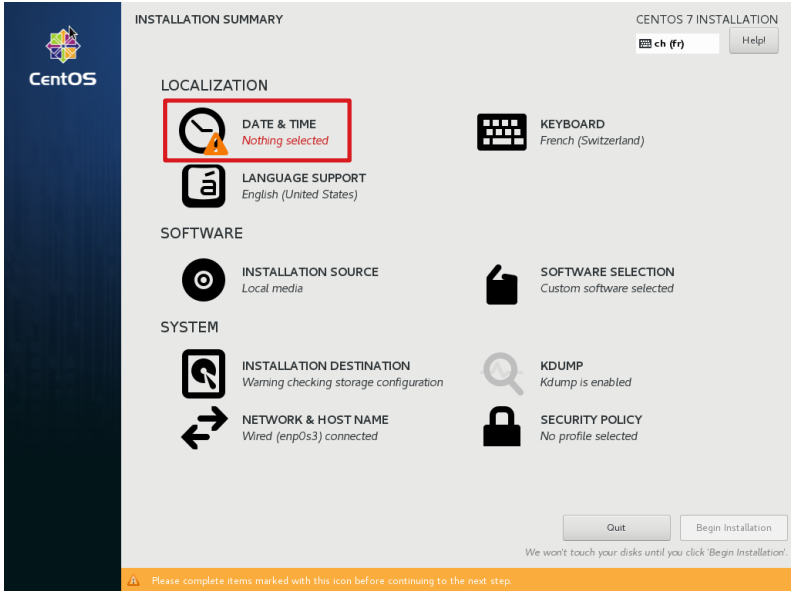
NG|OS Installation

- When started, VM will start on ISO file that has been mounted
- Welcome screen will appear
  - Type `ngscreener` to start install
- Anaconda installer will start
  - Semi automated install

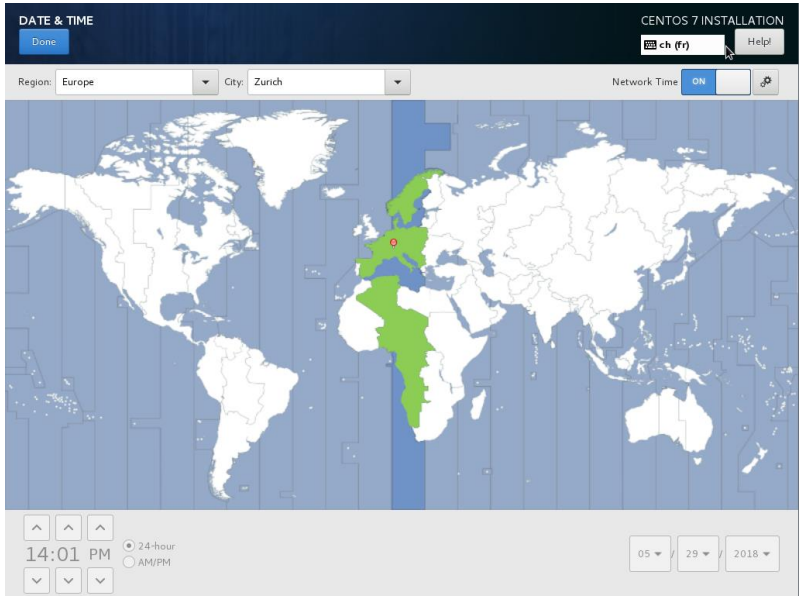


NG|OS Installation

Step 1: Anaconda Installer loaded, Click on Date & Time

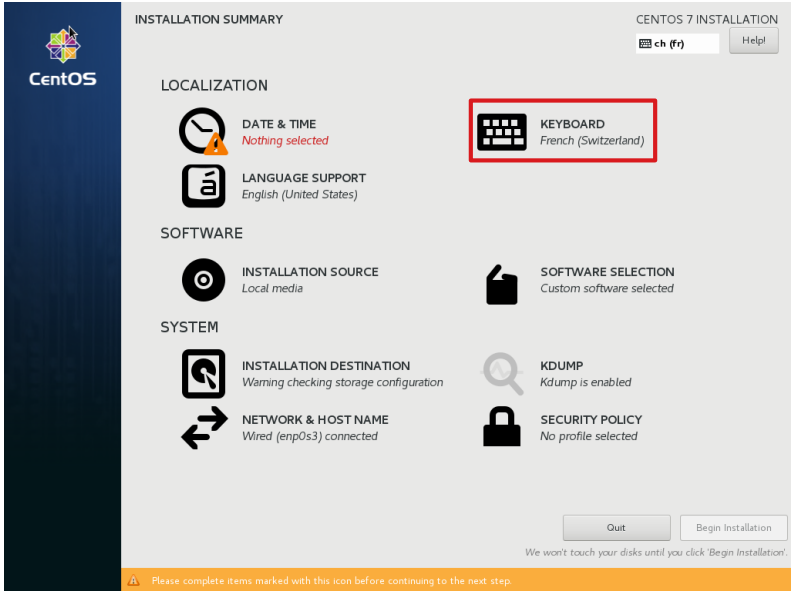


Step 2: Select correct timezone

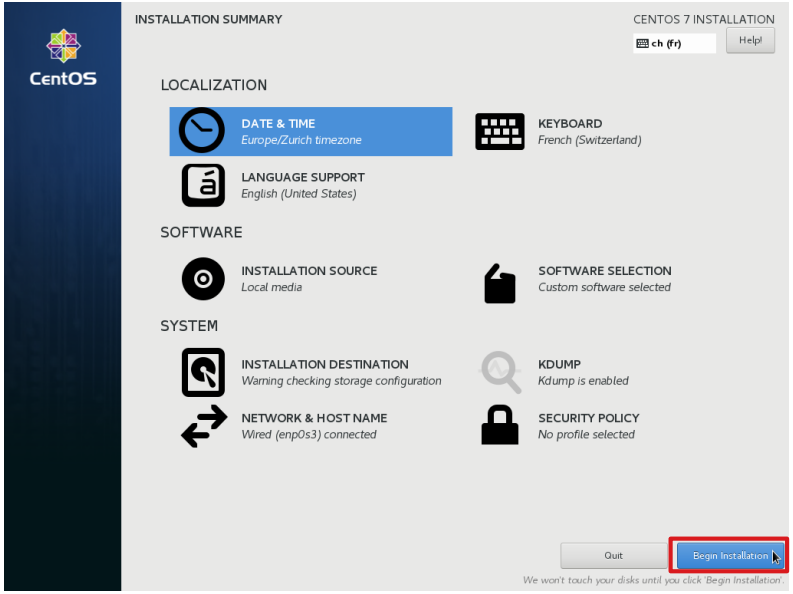


NG|OS Installation

Step 3: (Optional) Change keyboard layout

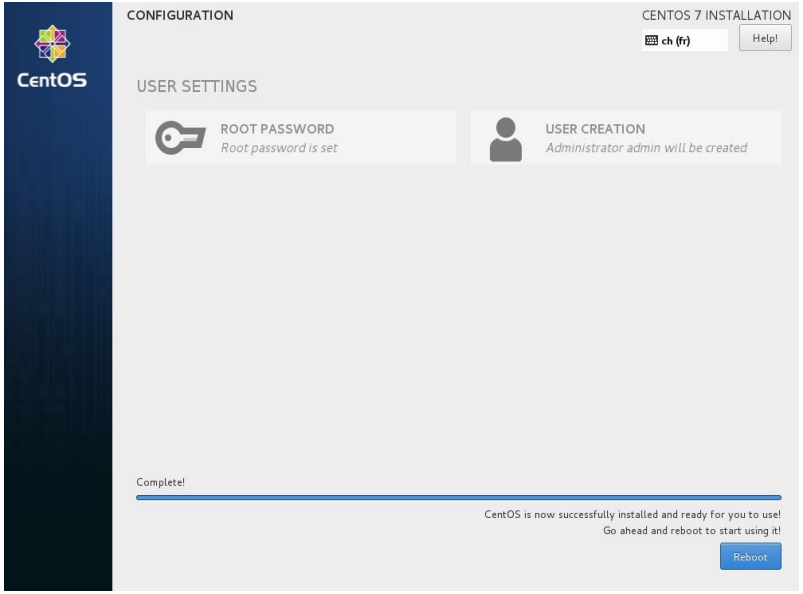


Step 4: Begin Installation (approx. 30 min)

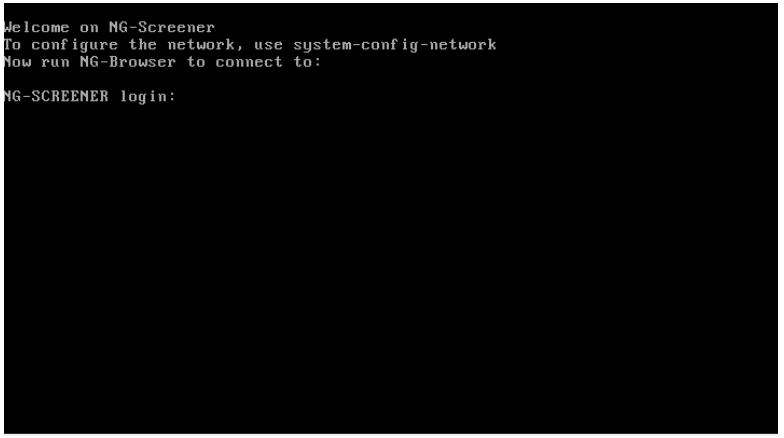


NG|OS Installation

Step 5: Reboot at the end of OS install and unmount ISO



Step 6: Connect with `admin` / `netguardians` credentials



NG|OS Installation

Step 7: Check IP address provided with `ifconfig`

```
NG-SCREENER login: admin
Password:
[admin@NG-SCREENER ~]$
[admin@NG-SCREENER ~]$
[admin@NG-SCREENER ~]$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.210.4.72  netmask 255.255.0.0  broadcast 10.210.255.255
        inet6 fe80::3678:1370:6fc9:2528  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:62:df:db  txqueuelen 1000  (Ethernet)
        RX packets 3898  bytes 326497 (318.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 203  bytes 21716 (21.2 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 24  bytes 4079 (3.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 4079 (3.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[admin@NG-SCREENER ~]$ _
```

Step 8: OS is ready for component installation

NetGuardians

NG|Screener Component Installation

swiss made software

Component Installation

Installation Order

1. NG|Storage
2. NG|Messaging
3. NG|Processing
4. NG|Syslog
5. NG|Auth
6. NG|Daemon
7. NG|UI
8. NG|Case Manager
9. NG|Management Center
10. NG|Connectors
11. …

Before starting Install

- Components are provided as RPM packages
- RPM should be transferred to VM using a File transfer tool
  - SCP / SFTP on port **22**
  - User: **admin** / Pass: **netguardians**
- RPM install should be done as root (su / sudo)
- Configure second interface (host-only)

Configure Second Interface

Interface configuration

- Edit `/etc/sysconfig/network-scripts/ifcfg-enp0s8`
- Configuration on the right →
- Restart network
  - sudo `systemctl restart network`
- Could use demolocal.netguardians.ch to access machine
  - Needed for NG|Auth
  - See end of slide deck for some other needed configuration for NG|Auth

```
NM_CONTROLLED=yes
BOOTPROTO=none
ONBOOT=yes
IPADDR=192.168.56.11
NETMASK=255.255.255.0
DEVICE=enp0s8
PEERDNS=no
ZONE=public
```

Component Installation

1. NG|Storage Installation

- Install command
  - `sudo rpm -ivh NgStorage-X.Y.Z.rpm`

- Post install actions
  - `sudo systemctl daemon-reload`
  - `sudo systemctl enable ng-storage.service`
  - `sudo systemctl start ng-storage.service`

- Post install check
  - RPM listed as installed: `rpm -qa NgStorage`
  - Service started: `sudo systemctl status ng-storage`

Component Installation

2. NG|Messaging Installation

- Install command
  - `sudo rpm -ivh ngMessaging-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa NgMessaging`
  - Service started:
    - `sudo systemctl status ng-messaging`
    - `sudo systemctl status ng-zookeeper`
    - `sudo systemctl status ng-kafka-manager`

Component Installation

3. NG|Processing Installation

- Install command
  - `sudo rpm -ivh NgProcessing-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa NgProcessing`
  - Service started:
    - `sudo systemctl status ng-history-server`
    - `sudo systemctl status ng-mesos-master`
    - `sudo systemctl status ng-mesos-slave`
    - `sudo systemctl status ng-thrift-server`

Component Installation

4. NG|Syslog Installation

- Install command
  - `sudo rpm -ivh ngSyslogNg-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngSyslogNg`
  - Service started:
    - `sudo systemctl status syslog-ng.ngc`

Component Installation

5. NG|Auth Installation

- Install command
  - `sudo rpm -ivh ngAuth-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngAuth`
  - Service started:
    - `sudo systemctl status ng-screener-auth.service`

Component Installation

6. NG|Daemon Installation

- Install command
  - `sudo rpm -ivh ngDaemonDistrib-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngDaemonDistrib`
  - Service started:
    - `sudo systemctl status ng-screener`

Component Installation

7. NG|UI Installation

- Install command
  - `sudo rpm -ivh ngBrowser-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngBrowser`
  - Service started:
    - `sudo systemctl status ng-screener-ui`

Component Installation

8. NG|Case Manager Installation

- Install command
  - `sudo rpm -ivh --force ngCaseManagerRpm-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngCaseManagerRpm`
  - Service started:
    - `sudo systemctl status ng-case-manager`

Component Installation

9. NG|Management Center Installation

- Install command
  - `sudo rpm -ivh --force ngManagementCenter-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngManagementCenter`
  - Service started:
    - `sudo /etc/init.d/management.ngc status`

Component Installation

Connectors - Preparation

- Transfer connectors archive files to VM
- Uncompress all connectors
  - `cd /PATH/TO/CONNECTORS`
  - `unzip “*.zip”`

Connector - Install

- Install of all connectors at once
- `sudo rpm -ivh */connector/connector-*.rpm`
- Check install
  - `rpm -qa connector*`
- `Restart UI`
  - `sudo systemctl restart ng-screener-ui`

Component Installation

[Optional] NG|Import Installation

- Install command
  - `sudo rpm -ivh ngImport-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngImport`
  - Command available: `sudo ngimport`

Component Installation

[Optional] NG|Polling System Installation

- Install command
  - `sudo rpm -ivh --force ngPollingSystem-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa ngPollingSystem`
  - Service started:
    - `sudo systemctl status polling-system (service not started since no configuration for polling)`

Component Installation

[Optional] NG|Scoring API

- Install command
  - `sudo rpm -ivh ngScoringApi-X.Y.Z.rpm`
  - `sudo rpm -ivh ngScoringApiUi-X.Y.Z.rpm`

- Post install check
  - RPM listed as installed: `rpm -qa | grep ngScoringApi`
  - Service started:
    - `sudo systemctl status ng-scoring-api`
    - `sudo systemctl status ng-scoring-api-ui`

NetGuardians

Specific Configuration for NG|Auth

swiss made software

NG|Auth specific configuration

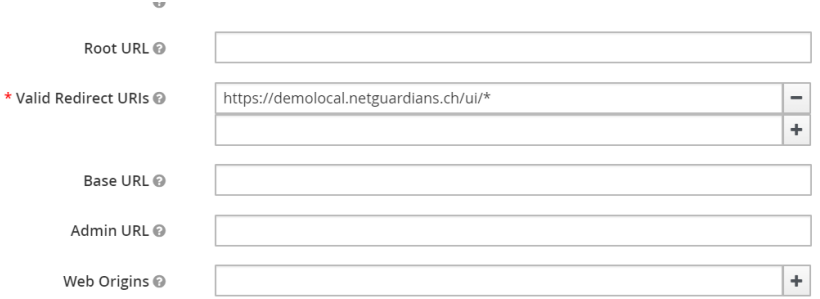
- Copy `apache_conf.zip` to VM
- Uncompress it and copy content to `/etc/httpd/conf.d/`
- Restart httpd service
  - `sudo systemctl restart httpd.ngc`
  - Careful there are two httpd services → Restart the one ending with .ngc (other is not started)

- Add to entries to /etc/hosts
  - `127.0.0.1 demolocal.netguardians.ch`
  - `192.168.56.11 demolocal.netguardians.ch`

- Add certs to keystore
  - `keytool -import -alias netguardians -file netguardians.crt -keystore /usr/java/latest/jre/lib/security/cacerts -storepass changeit -noprompt`
  - For both netguardians and intermediate certificates

NG|Auth specific configuration

- The URL should be now accessible:
  - https://demolocal.netguardians.ch/auth/admin
- Login with:
  - Username: `superadmin`
  - Password: `netguardians`
- Click on `clients` in the menu on the left
- Edit both `ngBrowser` and `ngCaseManager` client ID
  - Find option Valid Redirect URIs and change from `appliance.netguardians.ch` to `demolocal.netguardians.ch` (cf. printscreen).
  - Save your changes



NG|Auth specific configuration

- In command line, edit files in `/etc/ng-screener/common/auth/`
  - `DEFAULT_ngBrowser.json`
  - `DEFAULT_ngCaseManager.json`
- Modify parameter `auth-server-url` in both cases
  - `appliance.netguardians.ch` to `demolocal.netguardians.ch` (cf. printscreen)
- Restart both UI and Case Manager
  - `sudo systemctl restart ng-screener-ui`
  - `sudo systemctl restart ng-case-manager.ngc`

```
{
    "auth-server-url":
"https://demolocal.netguardians.ch/auth",
    "realm": "DEFAULT",
    "credentials": {
        "secret": "75db95d1-468b-420e-83ac-
d2bcde251113"
    },
    "verify-token-audience": true,
    "ssl-required": "external",
    "resource": "ngBrowser",
    "use-resource-role-mappings": true,
    "confidential-port": 0
}
```

*Refer to NG|Screener Install Guide chapter 3.9 about SSL configuration

NetGuardians

Check Installation

swiss made software

Check Installation

Sanity Check Script

- Execute at the end of installation of components
  - systemctl | grep -E "ngc-|ng-|-ng"

- `sudo python /usr/local/ng-screener/tools/sanity/sanity-check.py`

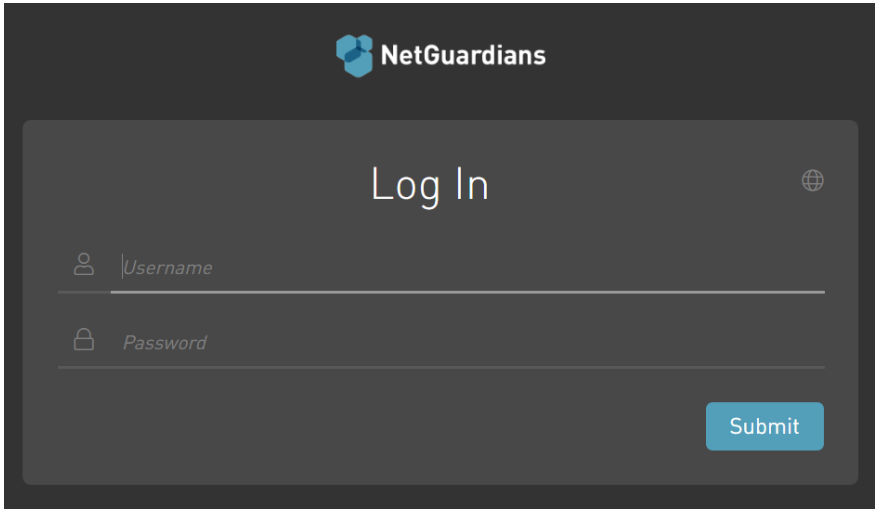
```
[admin@NG-SCREENER 03_Connectors]$ sudo python /usr/local/ng-screener/tools/sanity/sanity-check.py
Centos Version Check: OK
RAM Check: WRONG - Less than 8GB memory
Swap Check: OK
Check Partitions (/, /var/log, /data and /storage): OK
Check Databases Users OK
Check limits: OK
Check mariadb.ngc Service is running OK
Check licensing: OK
Check Java Version: OK
Check mysql2 is installed: OK
Check installed MariaDb packages: OK
Check if user ng-screener exists: OK
Check if /log-collector directory exists: OK
Check if ngStorage is installed: OK
Check if ng-storage.service is running: OK
Check ngStorage status: OK
```

Check Installation

Connect to Applications

- Accessing application through `https://demolocal.netguardians.ch`

- Credentials
  - User: `admin`
  - Pass: `netguardians`



THANK YOU!

Contact us

+41 24 425 97 60

info@netguardians.ch

www.netguardians.ch

Linkedin.com/company/netguardians

Facebook.com/NetGuardians

@netguardians

https://www.youtube.com/netguardians

NetGuardians Headquarters

Y-Parc, Av. des Sciences 13
1400 Yverdon-les-Bains
Switzerland

T +41 24 425 97 60
F +41 24 425 97 65

NetGuardians Africa

KMA Centre , 7th floor,
Mara Road Upper Hill,
Nairobi, Kenya

T +254 204 93 11 96

NetGuardians Asia

143 Cecil Street
#09-01 GB Building
069542 Singapore

T +65 6224 0987

NetGuardians
Eastern Europe

Koszykowa 61, 00-667
Warsaw, Poland

NetGuardians Germany

Rhein-Main Gebiet
Germany

T +49 172 3799003