1 Deploying the Appliance

The virtual appliance is provided by Greenbone in the Open Virtualization Appliance (OVA) format.
It requires and is limited to the following resources:

- 2 virtual CPUs
- 12 GB RAM
- 500 GB virtual hard disk

The following hypervisors are officially supported for running a OPENVAS BASIC.

- Microsoft Hyper-V, Server 2016, generation 2 virtual machine, VM configuration version 8.0 or higher
- VMware vSphere Hypervisor (ESXi), version 7.0 or higher
- VMware Workstation Player, version 17.0 or higher
- VMware Workstation Pro, version 17.0 or higher
- Oracle VirtualBox, version 7.0 or higher
- Huawei FusionCompute, version 8.0 (Intel only)

Please follow the instructions provided by the chosen hypervisor to deploy and start the appliance.

Note: The required booting mode is the EFI/UEFI boot mode.

After the appliance is started, log in using the default login information `admin:admin`. The password should be changed as soon as possible after the general system setup. The instruction can be found in the user manual.

2 Performing a General System Setup

When the appliance is set up initially, the GOS administration menu shows the first setup wizard after logging in to assist with the basic GOS configuration.

Configuring the Network

The network must be set up for the appliance to be fully functional. If there is no IP address configured, it is asked whether the network settings should be adjusted.

1. Select *Yes* and press `Enter`.
2. Select *Interfaces* and then the desired interface and press `Enter`.
3. If DHCP should be used, select *DHCP* (for IPv4 or IPv6) and press `Enter`.

or

3. If a static IP address should be used, select *Static IP* (for IPv4 or IPv6) and enter the IP address including the prefix length in the input box.
4. Select *Save* > *Back* > *Back* > *Ready*.

Generating an HTTPS certificate

An HTTPS certificate must be present on the appliance to use the web interface securely. To get started quickly, a self-signed certificate can be generated on the appliance itself. For enterprise use cases, users can also import their own SSL/TLS certificates that can authenticate their own domain.

1. Select *Generate* > *Continue*.
2. Provide the settings for the certificate.

   Note: It is valid to generate a certificate without a common name. However, a certificate should not be created without (a) Subject Alternative Name(s). If a common name is used, it should be the same as one of the SANs.

3. Select *OK* and press `Enter`.
   → A message informs that the certificate is created and can be downloaded. The download is not done now, but later in the GOS administration menu as described in the user manual.

Creating a Web Administrator

Since there is no web administrator yet, it is asked whether such an account should be created.

1. Select *Yes* and press `Enter`.
2. Enter the user name and the password for the web administrator.

   Note: For the user name, only all alphanumeric characters, - (dash), _ (underscore) and . (full stop) are allowed. The password can contain any type of character and can be at most 30 characters long.

3. Select *OK* and confirm the message by pressing `Enter`.

Finishing the Wizard and Logging in to the Web Interface

After the last step is finished, a status check is performed.

1. When the check is finished, press `Enter` to see the results.
2. Press `Enter` again to access the GOS administration menu. It can be used as described in the user manual.

The main user interface of the appliance is the web interface.

1. Open the web browser and enter the IP address of the appliance's web interface.

   Note: The web interface's IP address is displayed in the console login prompt or in the GOS administration menu when selecting *About* and pressing `Enter`.

2. Log in with the web administrator account created during the setup.

3 Configuring a First Scan

Note: All steps from Chapter 2 must be completed before continuing with the scan.

1. Select *Scans* > *Tasks* in the menu bar, move the cursor over in the upper left corner and select *New Task*.
2. Enter a name for the task.
3. For *Scan Targets*, click .
4. In the new dialog, enter a name for the target and a host to be scanned.

   Note: The IP address or the host name is required. In both cases it is necessary that the appliance can connect to the system. If using the host name, the appliance must also be able to resolve the name.

5. If an authenticated scan should be run, click for the desired credential type and create new credentials.
6. Save the credentials, the target, and then the task.
7. Click for the newly created task to run the scan.
   → The task is added to the waiting queue. Afterwards, the scanner begins with the scan.
   The report of a task can be displayed as soon as the task has been started by clicking the bar in the *Status* column. As soon as the status changes to *Done*, the complete report is available.