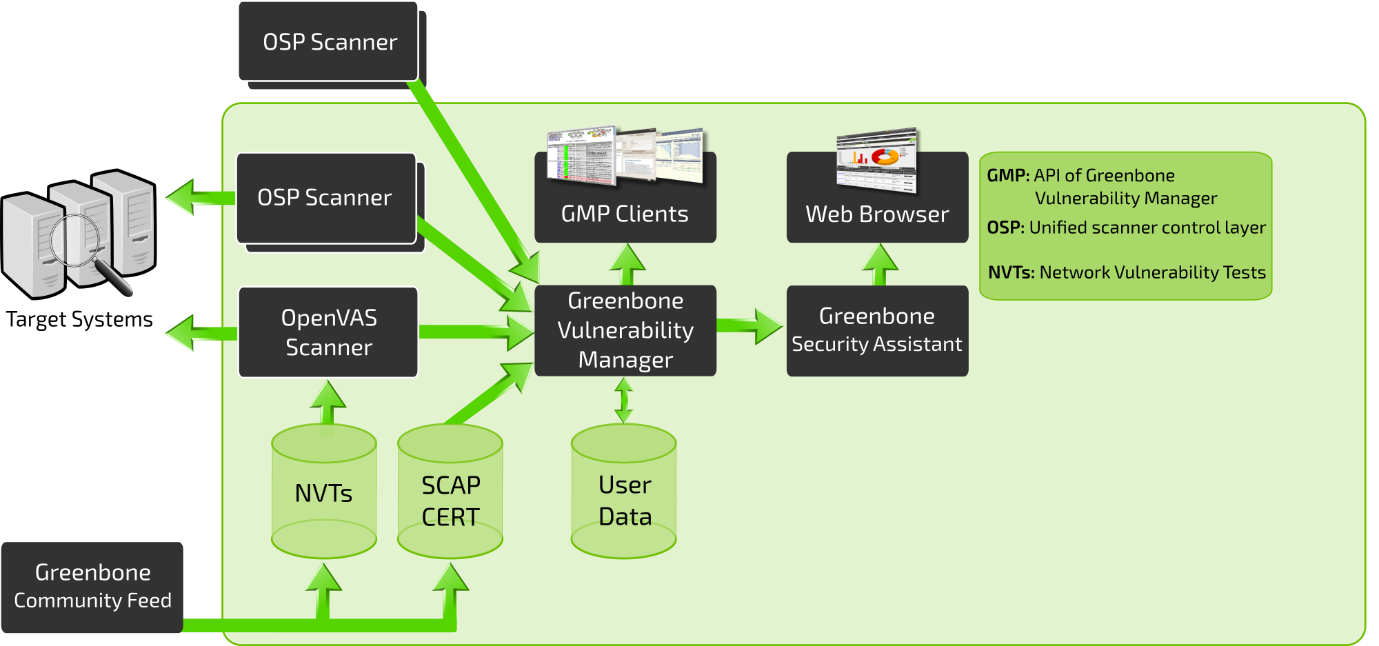
Greenbone Vulnerability Management Operating Instructions

Greenbone Vulnerability Management (GVM) is a network security scanner with associated tools like a graphical user front-end. The core component is a server with a set of network vulnerability tests (NVTs) to detect security problems in remote systems and applications. It is used by both offensive and defensive security experts to determine attack surface

GVM was previously known as Open Vulnerability Assessment System (OpenVAS). OpenVAS was a fork of Nessus, the popular corporate security scanner maintained by [Tenable](https://www.tenable.com). Both OpenVAS and Nessus were originally built from the [nmap](https://wiki.gentoo.org/wiki/Nmap) port scanner.

# Architecture

The Greenbone Vulnerability Management (GVM) is a framework of several services illustrated in the following architectural diagram:



## GVMd

The Greenbone Vulnerability Manager is the central service that consolidates plain vulnerability scanning into a full vulnerability management solution. GVMd controls the OpenVAS Scanner via an internal protocol and supports the generic [Open Scanner Protocol (OSP) 230](https://docs.greenbone.net/API/OSP/osp.html) for other scanner integrations.. GVMd also controls a PostgreSQL SQL database where all configuration and scan result data is centrally stored. Furthermore, GVMd also handles user management including permissions control with groups and roles. And finally the service has an internal runtime system for scheduled tasks and other events.

## GSA

The Greenbone Security Assistant is the web interface of GVM. It connects to the GVMd to provide a full-featured user interface for vulnerability management. Greenbone Security Assistant consists of

* GSA - The web application written in [React 43](https://reactjs.org/)
* GSAD - The HTTP server talking to the GVMd via GMP

## OpenVAS Scanner

The main scanner OpenVAS Scanner is a full-featured scan engine that executes a continuously updated and extended feed of Network Vulnerability Tests (NVTs). These NVT’s must be regularly updated (see section XXX)

# Installation

An image has been provided in the same location as these instructions. It is comprised of an OVF file and a VMDK file as follows:

packer-openvas.ovf

packer-openvas-disk001.vmdk

These files can be imported into VMWare using the standard import procedure

# Post Installation Steps

Once the VM has been imported and started the default passwords should be changed as follows:

8y$\*a$4.xX2aDY2

**Linux admin password**

ssh onto the VM using ubuntu/8y$\*a$4.xX<2aDY2 and run the following command:

passwd

Then input a suitable password.

**Web console password**

ssh onto the VM and run the following command :

gvmd --user=gvm --new-password=new\_password

How to setup cron job

## Definition updates

It is necessary to regularly update the feeds and NVT definitions to ensure the latest vulnerabilities are being scanned for. There is a script which is ran upon startup which will do this as follows:

/opt/gvm/updatedefs.sh

This can be ran on a regular basis by incorporating it into a cron job (note it must be ran as the gvm user). As an example (run every day at midnight):

echo "0 0 \* \* \* /opt/gvm/updatedefs.sh >> /opt/gvm/var/log/gvm/update.log" | crontab -

## Logging into via the front end

Access the instance at the following location

https://<server\_name>

Username : gvm

Password : 0p3nV@z

# Managing Certificates

The GSM appliance basically uses two types of certificates:

## Self-Signed Certificates

The use of self-signed certificates is the easiest way. It poses, however, the lowest security and more work for the user:

* The trustworthiness of a self-signed certificate can only be checked manually by the user through importing the certificate and examining its fingerprint.
* Self-signed certificates cannot be revoked. Once they are accepted by the user, they are stored permanently in the browser. If an attacker gains access to the corresponding private key a man-in-the-middle attack on the connection protected by the certificate can be launched.

This image already comes with a pre-installed certificate. The image comes with a self-signed certificate which means that when you access the GSM front end it will give a warning that the certificate cannot be validated and it is potentially unsafe to proceed. It is safe to click through this warning, however it is recommended that a proper certificate issued by a CA is used.

## Certificate by an External Certificate Authority (CA)

The use of a certificate issued by a CA has several advantages:

* All clients trusting the authority can verify the certificate directly and establish a security connection. No warning is displayed in the browser.
* The certificate can be revoked easily by the CA. If the clients have the ability to check the certificate status they can decline a certificate that may still be within its validity period but has been revoked. As mechanisms the Certificate Revocation Lists (CRLs) or Online Certificate Status Protocol (OCSP) can be used.
* Especially if multiple systems within an organization serve SSL/TLS protected information, the use of an organizational CA simplifies the management drastically. All clients simply have to trust the organizational CA to accept all the certificates issued by the CA.

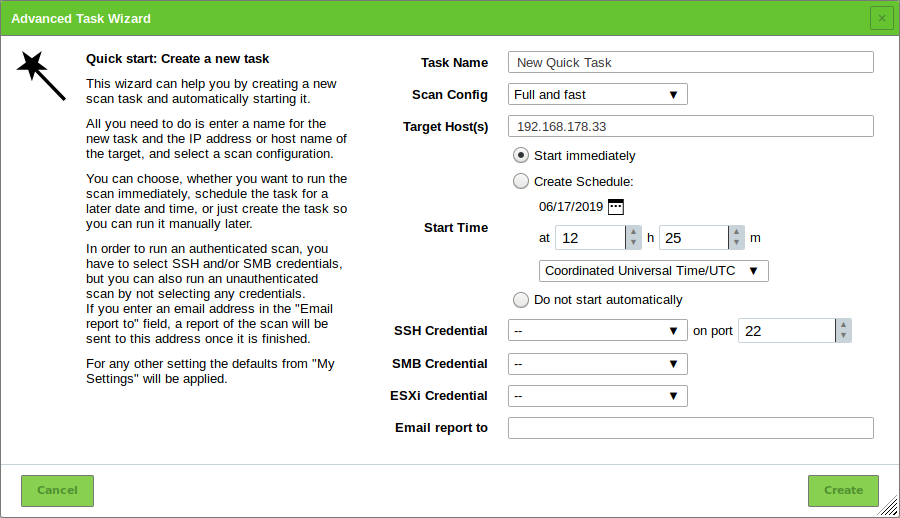
To import a certificate by an external CA two options are available:

* Generate a certificate signing request (CSR) on the GSM, sign it using an external CA and import the certificate.
* Generate a CSR and the certificate externally and import both using a PKCS#12 file.

# How to run a scan using the task wizard

A new task with the advanced task wizard can be configured as follows:

1. Select Scans > Tasks in the menu bar.
2. Start the wizard by moving the mouse over and clicking Advanced Task Wizard.
3. Define the task
4. If an e-mail address is entered in the input box Email report to an alert is created sending an e-mail as soon as the task is completed

[](https://docs.greenbone.net/GSM-Manual/gos-20.08/en/_images/adv_task_wizard.png)

1. Click Create.

→ The advanced task wizard performs the following steps automatically:

* 1. Starting the scan task immediately.
  2. Displaying the page Tasks.

## 10.3.1 Advantages and Disadvantages of Authenticated Scans

The extent and success of the testing routines for authenticated scans depend heavily on the permissions of the used account.

On Linux systems an unprivileged user is sufficient and can access most interesting information while especially on Microsoft Windows systems unprivileged users are very restricted and administrative users provide more results. An unprivileged user does not have access to the Microsoft Windows registry and the Microsoft Windows system folder \windows which contains the information on updates and patch levels.

Local security checks are the most gentle method to scan for vulnerability details. While remote security checks try to be least invasive as well, they may have some impact.

Simply stated an authenticated scan is similar to a Whitebox approach. The GSM has access to prior information and can access the target from within. Especially the registry, software versions and patch levels are accessible.

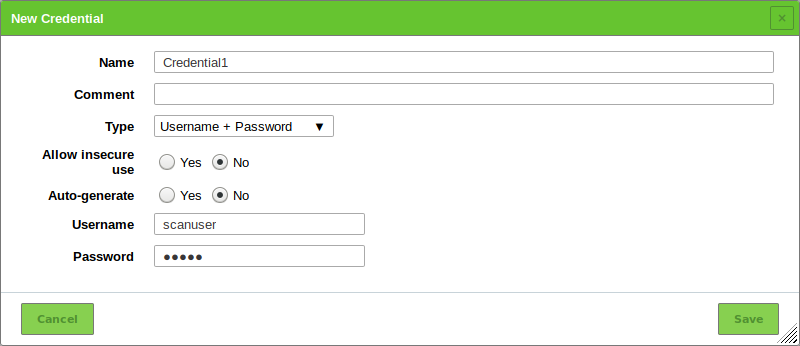
A remote scan is similar to a Blackbox approach. The GSM uses the same techniques and protocols as a potential attacker to access the target from the outside. The only information available was collected by the GSM itself. During the test the GSM may provoke malfunctions to extract any available information on the used software, e.g., the scanner may send a malformed request to a service to trigger a response containing further information on the deployed product.

During a remote scan using the scan configuration Full and fast all remote checks are safe. The used VTs may have some invasive components but none of the used VTs try to trigger a defect or malfunction in the target (see example below). This is ensured by the scan preference safe\_checks=yes in the scan configuration. All VTs with very invasive components or which may trigger a denial of service (DoS) are automatically excluded from the test.

# Creating a Credential

A new credential can be created as follows:

1. Select Configuration > Credentials in the menu bar.
2. Create a new credential by clicking the new button.
3. Define the credential

[](https://docs.greenbone.net/GSM-Manual/gos-20.08/en/_images/credential_new.png)

1. Click Save.

It is recommended that an account be created on the target machines specifically for conducting scans as opposed to using an existing account.

# Performing a Scheduled Scan

For continuous vulnerability management the manual execution of task is tedious. The GSM supports the scheduling of tasks for their automation and refers to schedules as automatic scans at a specific time. They can be run once or repeatedly.

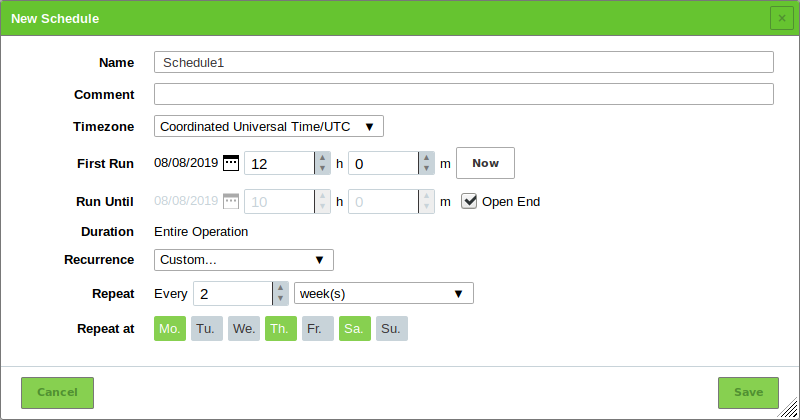
The GSM does not provide any schedules by default.

## Creating a Schedule

A new schedule can be created as follows:

1. Select Configuration > Schedules in the menu bar.
2. Create a new schedule by clicking the new button.
3. Define the schedule
4. Click Save.

→ The schedule is created and can be selected when creating a new task

[](https://docs.greenbone.net/GSM-Manual/gos-20.08/en/_images/schedule_new.png)

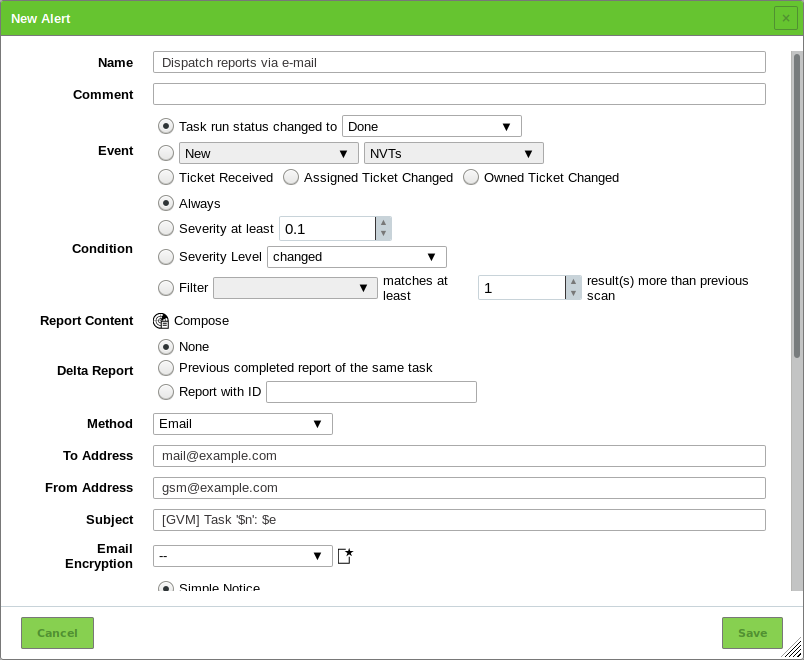
# Using Alerts

Alerts are anchored within the system. If a configured event (e.g., a task is finished) happens, a specified condition is checked (e.g., vulnerability with a high severity category detected). If the conditions is met, an action is performed, e.g., an e-mail is sent to a defined address.

## Creating an Alert

A new alert can be created as follows:

1. Select Configuration > Alerts.
2. Create a new alert by clicking the new button
3. Define the alert
4. Click Save.

[](https://docs.greenbone.net/GSM-Manual/gos-20.08/en/_images/alert_new.png)

Note in order to send email notifications an SMTP server must be configured.

# Further Reading

This document covers only the most basic setup - a comprehensive user guide can be found at the following location:

<https://docs.greenbone.net/GSM-Manual/gos-20.08/en/web-interface-access.html>