

# Using Pre-Scripts in VM Manager to patch GCP VMs (OS Patch Management)

**V**M Manager by GCP is no doubt absolutely a great tool that alleviates our overhead management of patching or OS Configuration with just a few clicks or `gcloud` commands. Today we are going to talk about [OS Patch Management](#) offering in [VM Manager](#).

Recently we'd a requirement of taking disk snapshots before monthly recurring patching got performed on our fleet of VMs, since GCP VM Manager as of now doesn't provide this capability in GUI or command line though we can achieve this via the pre-script option of OS Patch Manager.

## VM Manager

VM Manager is an offering from Google Cloud to manage and secure your Virtual Machine fleet(s). VM Manager is truly a valuable tool as managing and maintaining VM fleet(s) could be a totally challenging and lengthy task. VM Manager is a set or suite of tools for VM fleet management and it's here to save your day!

Right now, the following services are available as part of the VM Manager suite:

- [OS patch management](#)
- [OS inventory management](#)
- [OS configuration management](#)

## [VM Manager](#)

### **OS Patch Management**

Patch Manager is offering part of VM Manager that keeps your VMs up-to-date and protects it from any sort of vulnerabilities. Patch Manager works across Linux as well as for Windows-based VMs. It provides a detailed compliance report which provides insights on the patch status of your VM instances.

Patches can be applied via on-demand as well as scheduled along with pre and post-patch scripts that automate the OS and software patching. You can also perform a dry run of patching where your VMs get contacted though patching would not be performed.

You can leverage filters for flexible target VMs and could run patches (forcefully) on instances from MIGs too. Patch Manager also offers to exclude particular patches.

### [OS patch management \(Patch Manager\)](#)

### [How OS patch management works](#)

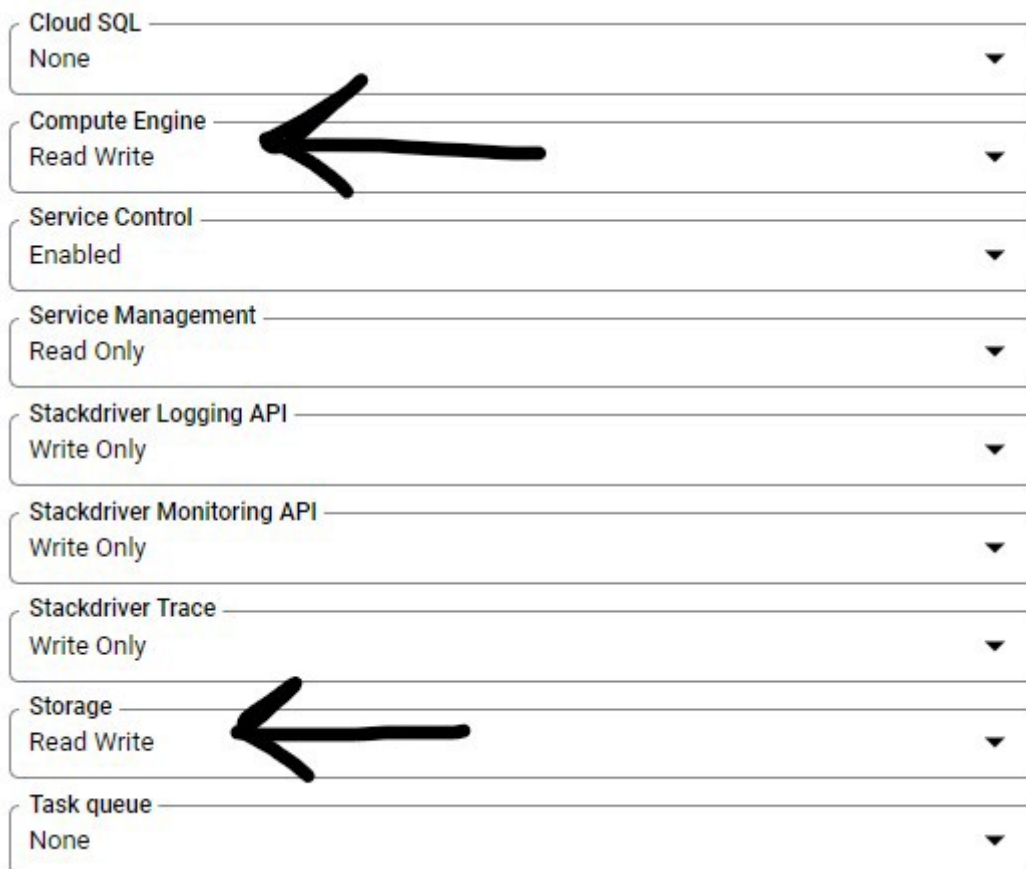
Scripts GitHub Repo Link:

<https://github.com/luvvero/gce-os-patch-mgt>

## Create Google Compute Engine Machine (GCE VM)

Let's create one Windows-based VM which needs to be patched.  
For this demo, we are creating one minimal VM with custom access [Set access for each API] to the service account with Read Write for Compute Engine and Storage API.

*Ignore the custom access line you've opted "Allow full access to all Cloud APIs".*



A screenshot of the Google Cloud Platform console showing the 'Custom access' section for a service account. The section contains a list of APIs with their respective access levels. Two arrows point to the 'Compute Engine' and 'Storage' rows, indicating the required 'Read Write' access.

API	Access
Cloud SQL	None
Compute Engine	Read Write
Service Control	Enabled
Service Management	Read Only
Stackdriver Logging API	Write Only
Stackdriver Monitoring API	Write Only
Stackdriver Trace	Write Only
Storage	Read Write
Task queue	None

Custom Access for Compute Engine and Storage API

If you have associated a custom service account with VM then add Compute Instance Admin `roles/compute.instanceAdmin` to SA however, if you've associated default SA no action is needed.

Add the following Custom Metadata to the VM

Key: enable-osconfig

Value: TRUE

Key: osconfig-log-level

Value: debug

By enabling osconfig-log-level to debug OS Config writes all logs to Cloud Logging and Serial port, this proves really helpful in case your scripts or patching are getting crashed or failed.

*Note: For connecting to Serial Port, you need to enable it for VMs.*

## Upload Scripts to GCS Bucket

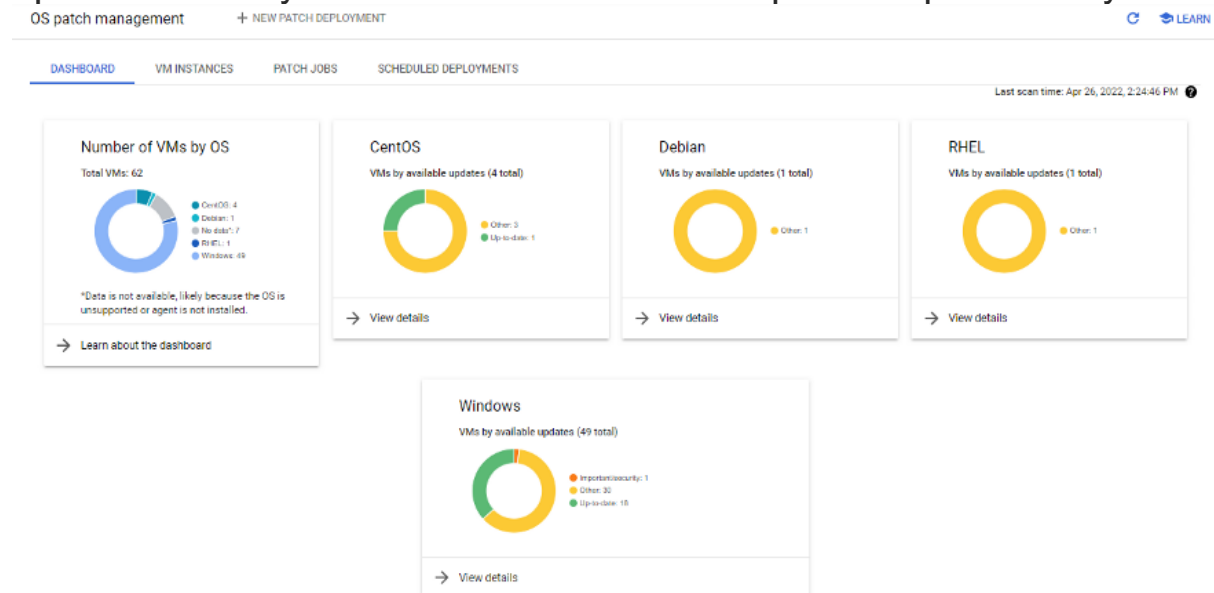
You need to upload your pre or post-patch-scripts to versioning enabled GCS Bucket which will be added on the last step while creating patch deployment.

Once you upload your script on GCS Bucket, get its versioning or generation number by running.

```
gsutil ls -a gs://GCS_BUCKET_NAME/script_name.ps1
```

## Setup Patch Management

Once you enable VM Manager API, it's time to set up VM Manager for VMs. You can choose to activate VM Manager either for all the VMs or selected VMs only, it totally depends on you. We have set it up automatically as our all VMs need to be patched periodically.



## OS Patch Management Dashboard

Wait for some time for VMs to appear on VM Manager Dashboard.

Now create a patch job for our Windows VM. This `gcloud` command creates an instantaneous patch for you and patch jobs are uneditable.

```
gcloud compute os-config patch-jobs execute \
  --instance-filter-names=zones/us-central1-a/instances/windows-vm-for-patching-1 \
  --display-name=windows-vm-patch \
  --duration=3600s \
  --reboot-config=default \
  --windows-classifications=critical,security,definition,driver,feature-pack,service-
pack,tool,update,update-rollup,update \
  --pre-patch-windows-executable=gs://vm-patch-scripts/windows-disk-
snapshot.ps1#1650968578616760 \
  --rollout-mode=zone-by-zone \
  --rollout-disruption-budget=1
```

To create recurring or run later patch job schedules you have to use either GCP UI Console or [gcloud compute os-config patch-deployments create](#) by providing a [JSON or YAML file](#) with patch deployment details. We don't prefer the latter.

The screenshot shows the 'Start patch deployment' form in the GCP UI Console. On the left, a sidebar lists five steps: 'Target VMs', 'Patch configuration', 'Scheduling' (which is selected and highlighted in blue), 'Rollout options', and 'Advanced options'. The main area is titled 'Start patch deployment' and contains several configuration options for a recurring schedule. The 'Recurring schedule' radio button is selected. Below it, there are five dropdown menus: 'Frequency \*' set to 'Monthly - On specific day', 'Select week \*' set to '3rd', 'Select day \*' set to 'Sunday', 'Enter time \*' set to '8:00 PM' with a time zone selector set to 'IST', and 'Days offset' set to '0'. At the bottom, there is a text input for 'Duration (maintenance window):' set to '60' minutes. A 'NEXT' button is located at the bottom right of the form.

✓ Target VMs

✓ Patch configuration

✓ Scheduling

4 Rollout options

5 Advanced options

### Start patch deployment

☐ Start now

☐ Schedule for later

☒ Recurring schedule

Frequency \*  
Monthly - On specific day

Select week \*  
3rd

Select day \*  
Sunday

Enter time \*  
8:00 PM IST

Days offset  
0

Duration (maintenance window):  
60 Minutes

NEXT

## Recurring Patch Deployment Schedule

### Script

Pre-patching or post-patching scripts run on the instance. The patch deployment wouldn't be executed if the pre-patch script fails.

*We have found a great PowerShell script written by [Christoph Petersen](#), Solution Lead, Google Cloud Platform EMEA*

on [GitHub](#) which was intended to create a disk clone before patching, we have modified it to our requirements accordingly.

Similarly, we have also modified this PowerShell script for creating Google Machine Image before patching VM and also added a disk cloning script.

## Verification & Explanation Boom Giphy

Once you execute the above `gcloud` command or hit Deploy on GCP UI, the patch job instantly (only for Start now) begins. Visit Patch Jobs to view the running job.

OS patch management [+ NEW PATCH DEPLOYMENT](#)

---

DASHBOARD VM INSTANCES **PATCH JOBS** SCHEDULED DEPLOYMENTS

Filter **windows** Enter property name or value

Job name	Start time ↓	End time	Targeted instances	Status	Dry run	Action
windows-vm-patch	Apr 26, 2022, 4:39:45 PM	Apr 26, 2022, 4:39:47 PM	0	Job executing	False	

### Patch Jobs

### Check for Snapshots.

**SNAPSHOTS** SNAPSHOT SCHEDULES

---

Filter **windows** Enter property name or value

<input type="checkbox"/>	Status	Name ↑	Location	Snapshot size	Creation time	Source disk	Disk size
<input type="checkbox"/>		windows-vm-for-patching-1-04262022110952	us	9.14 GB	Apr 26, 2022, 4:39:55 PM UTC+05:30	windows-vm-for-patching-1	50 GB

### Disk Snapshot

You can see the snapshot has been created successfully and now VM Manager will begin patching our Windows VM. We can see our patch job status in the VM Manager console.

Patch job execution details			
<a href="#">RE-RUN JOB</a> <a href="#">CANCEL</a>			
Result	Instances updated	Started on	Duration
Successfully completed	1	April 26, 2022 4:39 PM	1 hr

#### Update info

ID	d2d505f7-2850-4689-b7a2-86e3063f486c
Name	windows-vm-patch
State	SUCCEEDED
Percent complete	100%
Dry run	false
Error message	
Created	2022-04-26T11:09:45.571491Z
Updated	2022-04-26T11:12:19.019431Z
Duration	3600s
VM filter	
All VMs in project	false
Instances	1
Rollout	
Mode	Zone by zone
Number of VMs	1

## Patch Job Status

Likewise, we've run below PowerShell script for creating Google Machine Image before VMs are getting patched.

A machine image contains a VM's properties, metadata, permissions, and data from all its attached disks. You can use a machine image to create, backup, or restore a VM.  
[Learn more](#)

Filter Enter property name or value						
<input type="checkbox"/>	Status	Name ↑	Source instance	Machine type	Storage location	Creation time
<input type="checkbox"/>	✓	windows-vm-for-patching-1-05032022212335	windows-vm-for-patching-1	e2-medium	us-central1	May 3, 2022 5:03:20 PM UTC+05:30

Google Machine Image created before patching

Upon checking VM instances status from the Patch Manager dashboard you can see whether new updates are available or not.




## Basic info

Name	<a href="#">windows-vm-for-patching-1</a>
Zone	us-central1-a
OS distribution	Windows
OS version	Server 2019
Status	 Up-to-date
Last scan time	May 3, 2022, 8:55:56 PM

## Available updates

 Filter Enter property name or value 

Name 	Description	Categories	Published date
--	-------------	------------	----------------

No rows to display

[EQUIVALENT COMMAND LINE](#)

No further updates are available

*Note: Custom Image creation requires VM to be stopped and since pre-patch scripts run inside VMs, so it's not possible to create Custom Image. If there is any good solution is there, please highlight this line and comment.*

Scripts for Linux based VM are also present in [GitHub Repo](#).

Hope you enjoyed this blog, demonstrating the automation of the creation of disk snapshots and GMLs before Patching via VM Manager OS Patch Management which can really be a life-saver for the enterprises.

[VM Manager](#)

[OS Patch Management](#)

*Pre-Patch and Post-Patch Scripts*

*Script GitHub Link*