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

VM 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](https://cloud.google.com/compute/docs/os-patch-management)offering in [VM Manager](https://cloud.google.com/compute/docs/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](https://cloud.google.com/compute/docs/os-patch-management)
* [OS inventory management](https://cloud.google.com/compute/docs/instances/os-inventory-management)
* [OS configuration management](https://cloud.google.com/compute/docs/os-configuration-management)

[*VM Manager*](https://cloud.google.com/compute/docs/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)*](https://cloud.google.com/compute/docs/os-patch-management)

[*How OS patch management works*](https://cloud.google.com/compute/docs/os-patch-management#how_os_patch_management_works)

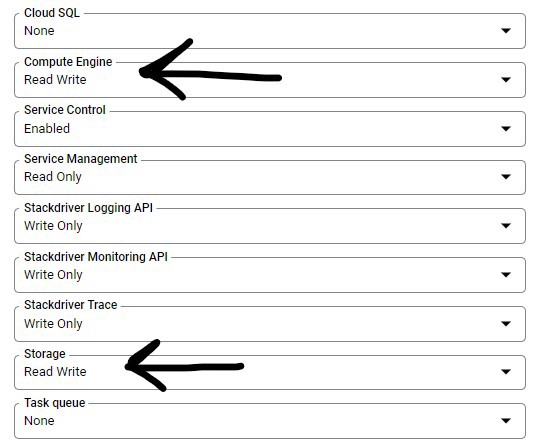
Scripts GitHub Repo Link:

<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”.*



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**

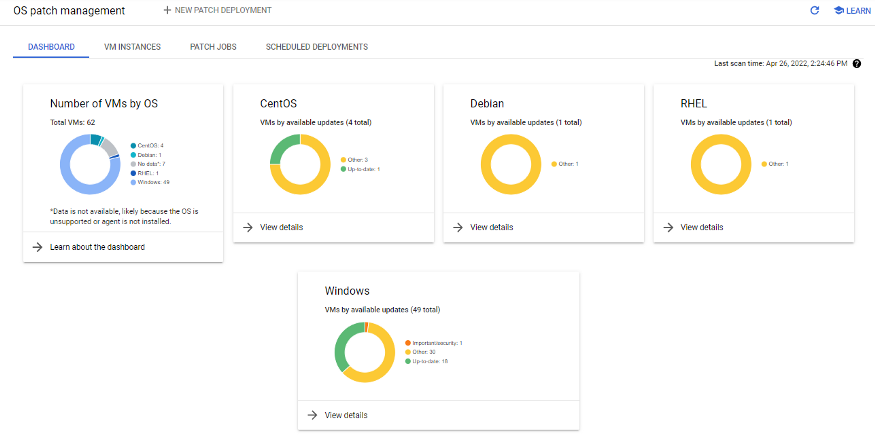
You need to upload your pre or post-patch-scripts to versioning enabled GCS Bucket which will be added on the last step while creating patch deployment.

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.



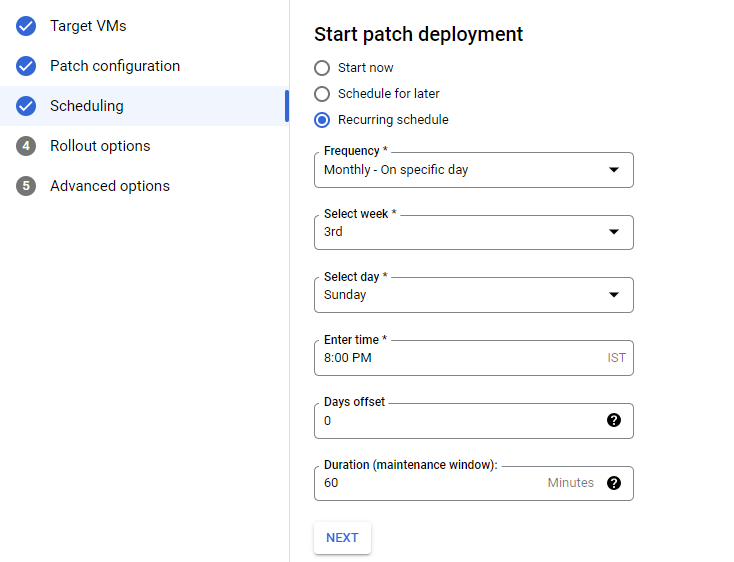
OS Patch Management Dashboard

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](https://cloud.google.com/sdk/gcloud/reference/compute/os-config/patch-deployments/create) by providing a [JSON or YAML file](https://cloud.google.com/compute/docs/osconfig/rest/v1/projects.patchDeployments) with patch deployment details. We don’t prefer the latter.



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.

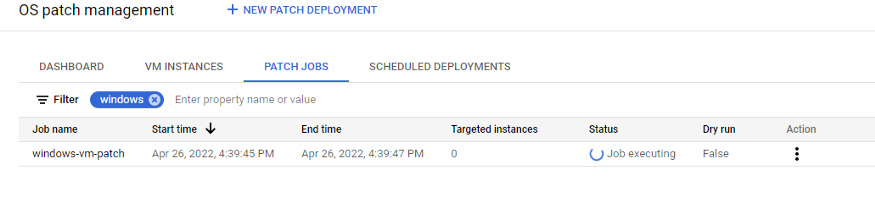
*We have found a great PowerShell script written by*[*Christoph Petersen*](https://github.com/peterschen)*, Solution Lead, Google Cloud Platform EMEA on*[*GitHub*](https://github.com/peterschen/blog/tree/master/gcp/samples/ospatch-clone)*which was intended to create a disk clone before patching, we have 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**

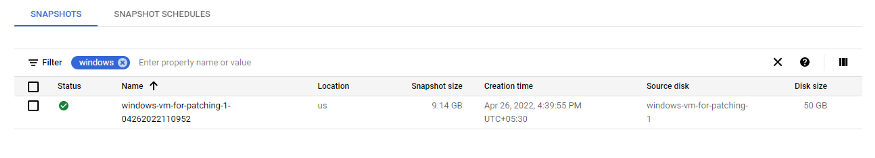
**Boom Giphy**

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.



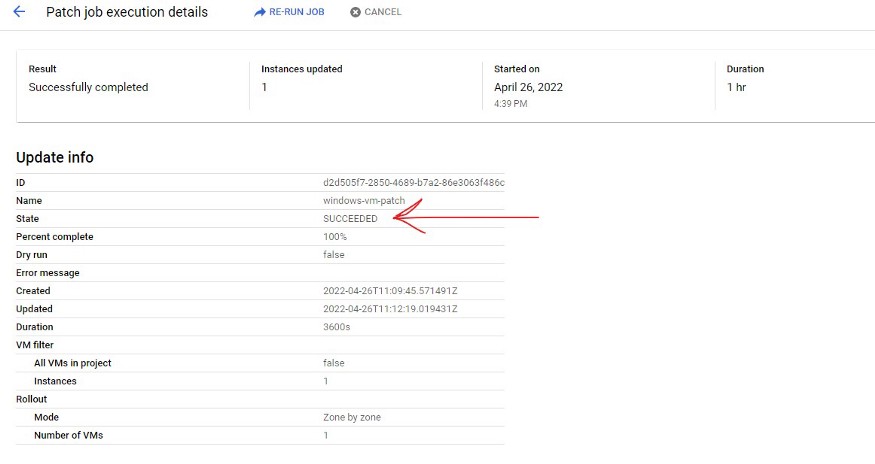
Patch Jobs

Check for Snapshots.



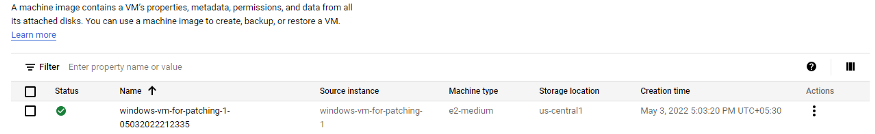
Disk Snapshot

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.



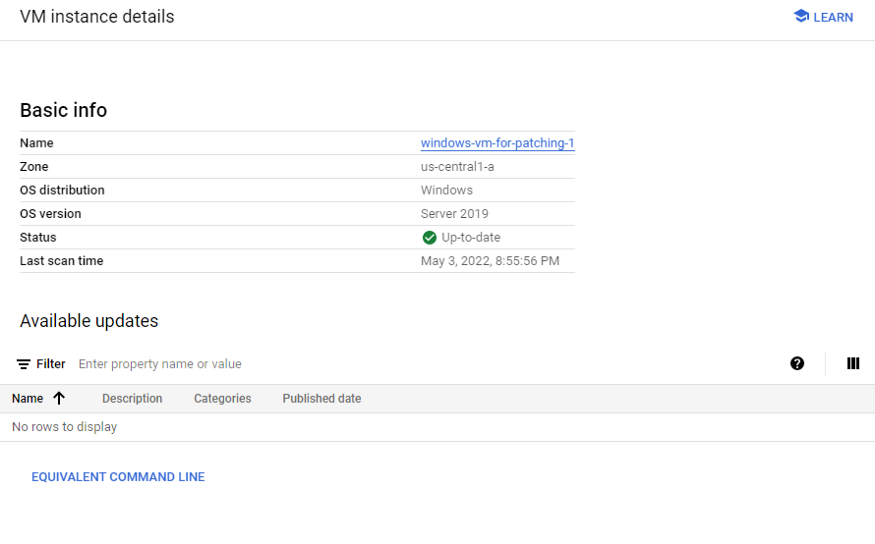
Patch Job Status

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



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.



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](https://github.com/luvvero/gce-os-patch-mgt).

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

[*VM Manager*](https://cloud.google.com/compute/docs/vm-manager)

[*OS Patch Management*](https://cloud.google.com/compute/docs/os-patch-management)

[*Pre-Patch and Post-Patch Scripts*](https://cloud.google.com/compute/docs/os-patch-management/create-patch-job?&_ga=2.25491007.-341082545.1649140533#add-scripts)

[*Script GitHub Link*](https://github.com/luvvero/gce-os-patch-mgt)