OS patch management

This page describes OS patch management and how it works. To create patch jobs, see Creating patch jobs pute/docs/os-patch-management/create-patch-job).

Use OS patch management to apply operating system patches across a set of Compute Engine VM instances (VMs). Long running VMs require periodic system updates to protect against defects and vulnerabilities.

The OS patch management service has two main components:

- Patch compliance reporting, which provides insights on the patch status of your VM instances across Windows and Linux distributions. Along with the insights, you can also view recommendations for your VM instances.
- Patch deployment, which automates the operating system and software patch update process. A *patch deployment* schedules *patch jobs*. A *patch job* runs across VM instances and applies patches.

Benefits

The OS patch management service gives you the flexibility to complete the following processes:

- Create patch approvals. You can select what patches to apply to your system from the full set of updates available for the specific operating system.
- Set up flexible scheduling. You can choose when to run patch updates (one-time and recurring schedules).
- Apply advanced patch configuration settings. You can customize your patches by adding configurations such as pre and post patching scripts.
- Manage these patch jobs or updates from a centralized location. You can use the the OS patch management dashboard (#dashboard) for monitoring and reporting of patch jobs and compliance status.

Pricing

OS Patch management is free of charge from now through December 31st, 2020. Starting January 1, 2021, OS patch management will incur charges per the number of VMs that have the OS Config agent running as follows:

- OS Patch management is free of charge for the first 100 VMs that have the OS Config agent running.
- For all additional VMs that have the OS Config agent running, each agent is charged at a rate of $0.003 per hour per VM (roughly $2 per month per VM).

How OS patch management works

To use the OS patch management feature, you must set up the OS Config API and install the OS Config agent. For detailed instructions, see Setting up OS Config (/compute/docs/manage-os). The OS Configuration service enables patch management in your environment while the OS Configuration agent uses the update mechanism for each operating system to apply patches. Updates are pulled from the package repositories (otherwise called the *distribution source package*) or a local repository for the operating system.

The following table summarizes the update tool and distribution source packages that are used to collect data.

Operating system	Update tool	Distribution source package
RHEL and Centos	**`yum upgrade`**	• https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL6.xml (https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL6.xml) • https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml (https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL7.xml) • https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml (https://www.redhat.com/security/data/oval/com.redhat.rhsa-RHEL8.xml)
Debian	**`apt upgrade`**	https://security-tracker.debian.org/tracker/data/json (https://security-tracker.debian.org/tracker/data/json)

Operating system	Update tool	Distribution source package
Ubuntu	`apt upgrade`	https://storage.googleapis.com/ubuntu-cve-tracker/ubuntu.tar.gz (https://storage.googleapis.com/ubuntu-cve-tracker/ubuntu.tar.gz)
Windows	Windows Update Agent	Windows Update service, or the local Windows Server Update Service (WSUS)

If your VM does not have access to the updates, you must complete additional steps to allow access to the updates or patches. Consider the following options:

- Google recommends hosting your own local repository or a Windows Server Update Service for full control over the patch baseline.
- Alternatively, you can make external update sources available to your VMs by using Cloud NAT (/nat/docs/using-nat) or other proxy services.

Patch management consist of two services: patch deployment and patch compliance. Each of service is explained in the following sections.

Patch deployment overview

A patch deployment is initiated by making a call to the Patch API (also known as the Cloud OS Config API). This can be done by using either the Google Cloud Console, `gcloud` command-line tool, or a direct API call. Then the Patch API notifies the OS Config agent that is running on the target VMs to start patching.

The OS Config agent runs the patching on each VM by using the patch management tool that is available for each distribution. For example, Ubuntu VMs use the `apt` utility tool. The utility tool retrieves updates (patches) from the distribution source for the operating system. As patching proceeds, the OS Config agent reports the progress to the Patch API.

Patch compliance overview

After you set up OS Config (/compute/docs/manage-os) on a VM, the following takes place on the VM:

- The OS Config agent periodically (about every 10 minutes) reports OS inventory data (/compute/docs/instances/os-inventory-management#data-collected) into guest attributes (/compute/docs/storing-retrieving-metadata#guest_attributes) for the VM.
- The patch compliance backend periodically reads this data, cross references it with the package metadata obtained from the OS distribution, and saves it in the Container Analysis service (/container-registry/docs/metadata-storage) repository.
- The Google Cloud Console then gets the patch compliance data from the Container Analysis API service and displays this information in the console.

How patch compliance data is generated

The patch compliance backend periodically completes the following tasks:

1. Reads the reports that are collected from OS inventory data (/compute/docs/instances/os-inventory-management#data-collected) on a VM.
2. Scans for classification data from the distribution source for each operating system, and orders this data based on severity (from highest to lowest).
3. Maps these classifications (provided by the distribution source) to Google's patch compliance status (/compute/docs/os-patch-management#patch_compliance_status).
4. Saves the data in the Container Analysis service (/container-registry/docs/metadata-storage) repository.
5. Selects the highest severity data for each available update and shows it on the Google Cloud Console dashboard page. You can also see a full report of all available updates for the VM on the VM details page (/compute/docs/os-patch-management/manage-patch-jobs#list-instance-details).

The following table summarizes the mapping system used to generate Google's patch compliance status.

Distribution source categories	Google's patch compliance status
• Critical • Urgent • WINDOWS_CRITICAL_UPDATE	Critical (RED)

Distribution source categories	Google's patch compliance status
• Important • High • WINDOWS_SECURITY_UPDATE	Important/Security (ORANGE)
• Everything else	Other (YELLOW)
• No updates available	Up-to-date (GREEN)

For example, if the OS inventory data (/compute/docs/instances/os-inventory-management#data-collected) for a RHEL 7 VM has the following package data:

- Package name: package1
- Installed Version: 1.4
- Update Version: 2.0

The patch compliance backend scans for classification data (from the source distribution) and retrieves the following information:

- Version 1.5 => Critical
- Version 1.8 => Low
- Version 1.9 => Low

Then on the Google Cloud Console dashboard, this RHEL 7 VM is then added to list of VMs that have a `Critical` update available. If you review the details for this VM, you see 1 `Critical` update and 2 `Low` updates available.

Simultaneous patching

When you initiate a patch job, the service uses the instance filter (/compute/docs/os-patch-management/create-patch-job#instance-filters) you provided to determine the specific instances to be patched. Instance filters allow you to simultaneously patch many instances at the same time. This filtering is done when the patch job starts to account for changes in your environment after the job is scheduled.

Scheduled patching

Patches can be executed on demand, scheduled in advance, or configured with a recurring schedule. You can also cancel an in-progress patch job if you need to stop it immediately.

In the event of a cancellation or timeout, the OS Config agent attempts to complete the task it is on before stop

You can set up patch maintenance windows by creating patch deployments with a specified frequency and duration. Scheduling patch jobs with a specified duration ensures that patching tasks do not start outside of your designated maintenance window.

You can also enforce patch installation deadlines by creating patch deployments to be completed at a specific time. If targeted VMs are not patched by this date, then the scheduled deployment starts installing patches on this date. If VMs are already patched no action is taken on those VMs, unless a pre or post patch script is specified or a reboot is required.

What is included in an OS patch job?

When a patch job runs on a VM, depending on the operating system, a combination of updates are applied. You can also choose to target specific updates, packages, or, for Window operating systems, specify the KB IDs that you want to update.

WindowsRHEL/CentOS (#rhelcentos)**Debian/Ubuntu** (#debianubu… **SUSE** (#suse)

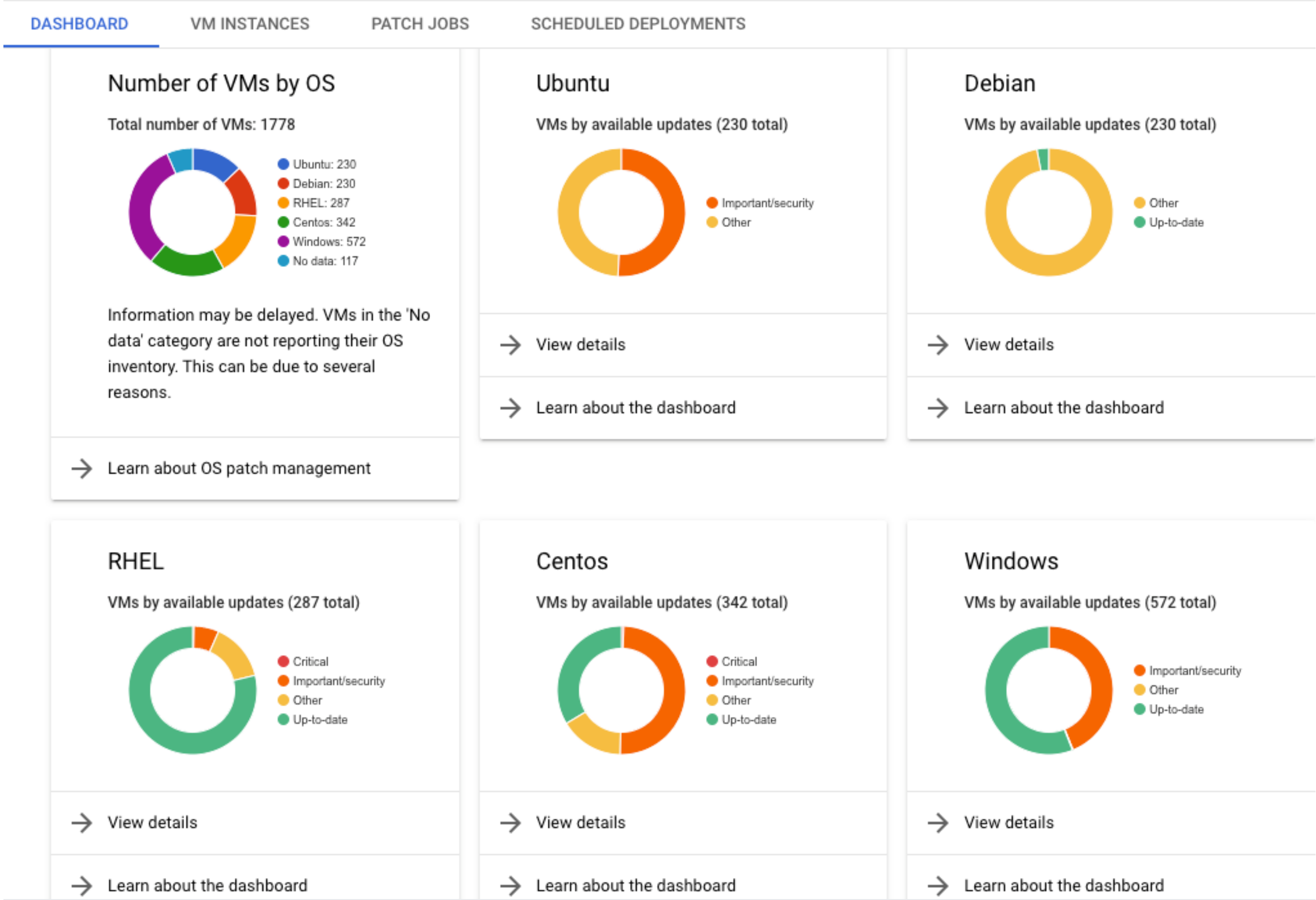
For Windows operating system, you can apply all or select from the following updates:

- Definition updates
- Driver updates
- Feature pack updates
- Security updates
- Tool updates

The OS patch management dashboard

In the Google Cloud Console, a dashboard is available that you can use to monitor the patch compliance for your VM instances.

Go to the OS Patch Management page (https://console.cloud.google.com/compute/patch)



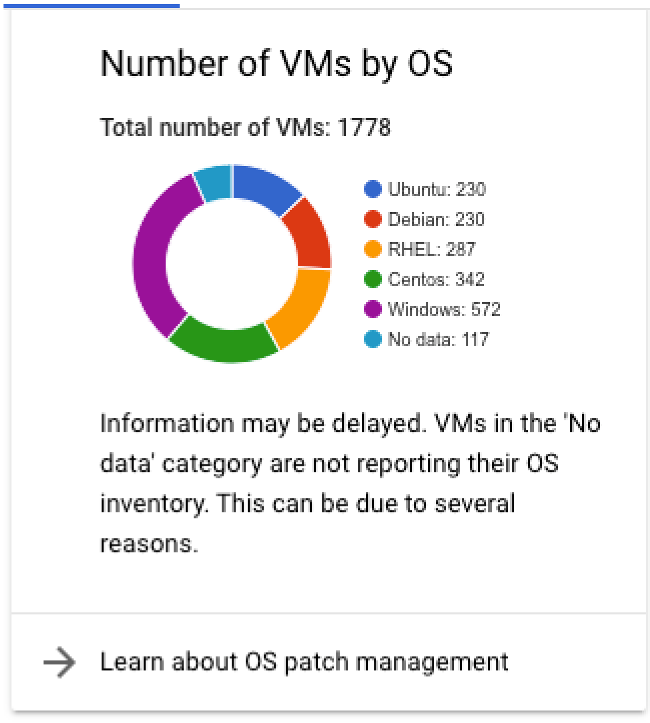
Information may be delayed. VMs in the 'No data' category are not reporting their OS inventory. This can be due to several reasons.

(https://cloud.google.com/compute/images/manage-os/os-patchdashboard.png)

Understanding the OS patch management dashboard

Operating system overview

This section reflects the total number of VMs, organized by operating system. For a VM to show up in this list, it must have the OS Config agent installed (/compute/docs/manage-os#check-install) and OS inventory management enabled (/compute/docs/manage-os#enable-metadata).



Number of VMs by OS

Total number of VMs: 1778

Information may be delayed. VMs in the 'No data' category are not reporting their OS inventory. This can be due to several reasons.

→ Learn about OS patch management

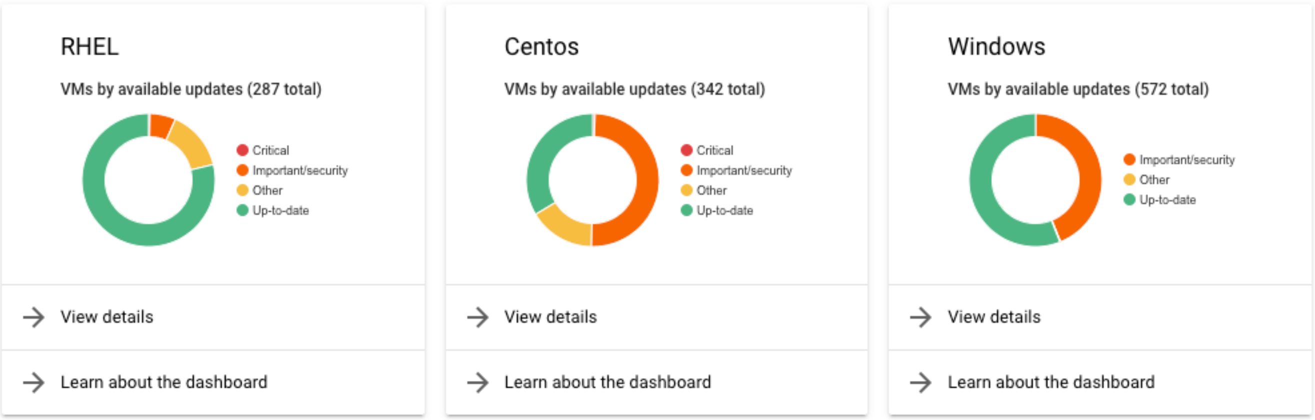
(https://cloud.google.com/compute/images/manage-os/number-of-vms.png)

If a VM is listed with its operating system as `No data`, one or more of the following scenarios might be true:

- The VM is unresponsive.
- OS Config agent is not installed.
- OS inventory management is not enabled.
- The operating system is not supported. For a list of supported operating systems, see Supported operating systems (/compute/docs/os-patch-management/create-patch-job#supported_operating_systems).

★ **Note:** For all supported SUSE Enterprise Linux Server (SLES) operating systems (including SLES for SAP and openSuse), you can run patch jobs (/compute/docs/os-patch-management/create-patch-job) and create patch deployments (/compute/docs/os-patch-management/schedule-patch-jobs). However, patch compliance reporting is not supported on SLES and the VMs are displayed in the **`No data`** category on the OS patch management dashboard.

Patch compliance status



(https://cloud.google.com/compute/images/manage-os/os-specific.png)

This section provides details of the compliance status of each of the VMs organized by their operating system.

Compliance status are arranged in four main categories:

- Critical: This means that a VM has critical updates available.
- Important or security: This means that a VM has important or security updates available.
- Other: This means that a VM has updates available, but none of these updates are categorized as a critical or security update.
- Up-to-date: This means that a VM has no updates available.

What's next?

- Create a patch job (/compute/docs/os-patch-management/create-patch-job).
- Manage patch jobs (/compute/docs/os-patch-management/manage-patch-jobs).
- Schedule patch jobs (/compute/docs/os-patch-management/schedule-patch-jobs).

Last updated 2020-08-19 UTC.