

Hotpatch for virtual machines

Article • 10/10/2023

Hotpatching is a way to install OS security updates on supported *Windows Server Datacenter: Azure Edition* virtual machines (VMs) that doesn't require a reboot after installation. It works by patching the in-memory code of running processes without the need to restart the process. This article covers information about hotpatch for supported VMs, which has the following benefits:

- Fewer binaries mean update install faster and consume less disk and CPU resources.
- Lower workload impact with fewer reboots.
- Better protection, as the hotpatch update packages are scoped to Windows security updates that install faster without rebooting.
- Reduces the time exposed to security risks and change windows, and easier patch orchestration with Azure Update Manager.

Supported platforms


Hotpatch is supported only on VMs and Azure Stack HCI created from images with the exact combination of publisher, offer and sku from the below OS images list. Windows Server container base images or Custom images or any other publisher, offer, sku combinations aren't supported.

Publisher	OS Offer	Sku
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Core-smalldisk
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch
MicrosoftWindowsServer	WindowsServer	2022-Datacenter-Azure-Edition-Hotpatch-smalldisk


To get started using Hotpatch, use your preferred method to create an Azure or Azure Stack HCI VM, and select one of the following images that you would like to use. Hotpatch is selected by default when creating an Azure VM in the Azure portal.

- Windows Server 2022 Datacenter: Azure Edition Hotpatch (Desktop Experience)
- Windows Server 2022 Datacenter: Azure Edition Core¹

¹ Hotpatch is enabled by default on Server Core images.

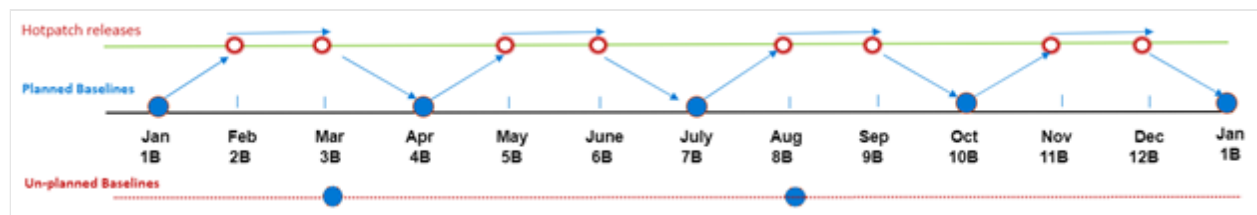
For more information about the available images, see the [Windows Server 2022 Datacenter](#)  Azure Marketplace product.

How Hotpatch works

Hotpatch works by first establishing a baseline with the current Cumulative Update for Windows Server. Periodically (starting every three months), the baseline is refreshed with the latest Cumulative Update, then hotpatches are released for two months following. For example, if January is a Cumulative Update, February and March would be a hotpatch release. For the hotpatch release schedule, see [Release notes for Hotpatch in Azure Automanage for Windows Server 2022](#) .

Hotpatches contains updates that don't require a reboot. Because Hotpatch patches the in-memory code of running processes without the need to restart the process, your applications are unaffected by the patching process. This action is separate from any potential performance and functionality implications of the patch itself.

The following image is an example of an annual three-month schedule (including example unplanned baselines due to zero-day fixes).



There are two types of baselines: **Planned baselines** and **Unplanned baselines**.

- **Planned baselines** are released on a regular cadence, with hotpatch releases in between. Planned baselines include all the updates in a comparable *Latest Cumulative Update* for that month, and require a reboot.
 - The sample schedule illustrates four planned baseline releases in a calendar year (five total in the diagram), and eight hotpatch releases.
- **Unplanned baselines** are released when an important update (such as a zero-day fix) is released, and that particular update can't be released as a hotpatch. When unplanned baselines are released, a hotpatch release is replaced with an unplanned baseline in that month. Unplanned baselines also include all the updates in a comparable *Latest Cumulative Update* for that month, and also require a reboot.
 - The sample schedule illustrates two unplanned baselines that would replace the hotpatch releases for those months (the actual number of unplanned baselines in a year isn't known in advance).

Supported updates

Hotpatch covers Windows Security updates and maintains parity with the content of security updates issued to in the regular (nonhotpatch) Windows update channel.

There are some important considerations to running a supported *Windows Server Azure Edition* VM with hotpatch enabled. Reboots are still required to install updates that aren't included in the hotpatch program. Reboots are also required periodically after a new baseline has been installed. Reboots keep the VM in sync with nonsecurity patches included in the latest cumulative update.

- Patches that are currently not included in the hotpatch program include non security updates released for Windows, .NET updates and non-Windows updates (such as drivers, firmware update etc.). These types of patches may need a reboot during Hotpatch months.

Patch orchestration process

Hotpatch is an extension of Windows Update and typical orchestration processes. Patch orchestration tools vary depending on your platform. To orchestrate Hotpatch:

- **Azure:** Virtual machines created in Azure are enabled for [Automatic VM Guest Patching](#) by default with a supported *Windows Server Datacenter: Azure Edition* image. Automatic VM guest patching in Azure:
 - Patches classified as Critical or Security are automatically downloaded and applied on the VM.
 - Patches are applied during off-peak hours in the VM's time zone.
 - Azure manages patch orchestration and patches are applied following [availability-first principles](#).
 - Virtual machine health, as determined through platform health signals, is monitored to detect patching failures.

ⓘ Note

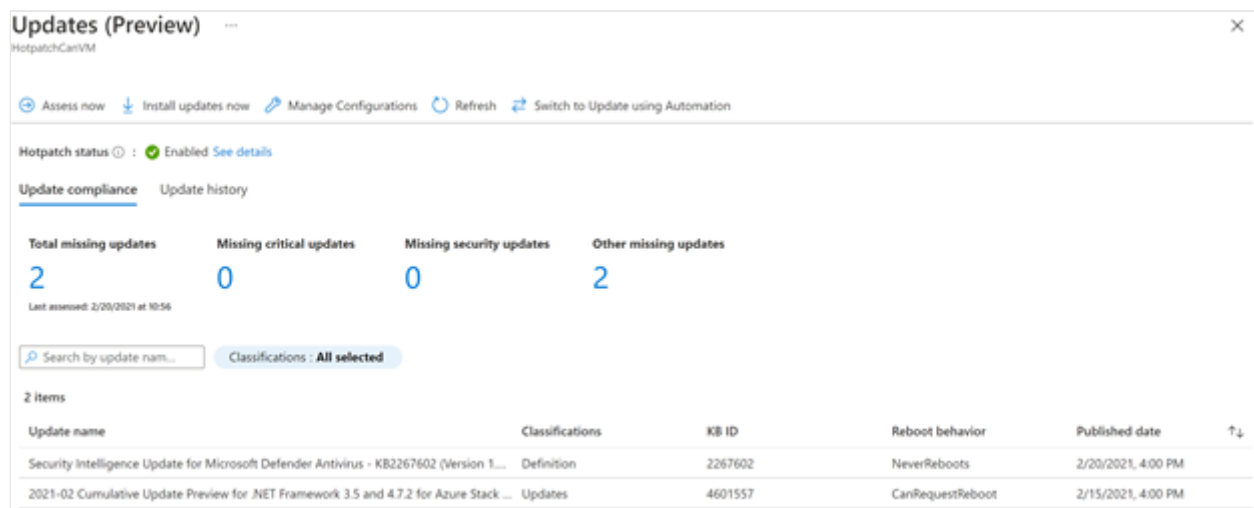
You can't create VM scale sets (VMSS) with Uniform orchestration on Azure Edition images with Hotpatch. To learn more about which features are supported by Uniform orchestration for scale sets, see [A comparison of Flexible, Uniform, and availability sets](#).

- **Azure Stack HCI:** Hotpatch updates for virtual machines created on Azure Stack HCI are orchestrated using:
 - Group Policy to configure the Windows Update client settings.
 - Configuring Windows Update client settings, or SCONFIG for Server Core.
 - A third-party patch management solution.

Understand the patch status for your VM in Azure

To view the patch status for your VM, browse to the VM Overview in the Azure portal, under Operations, select **Updates**. Under the **Recommended updates** section, you can view the latest patches and Hotpatch status for your VM.

On this screen, you see the hotpatch status for your VM. You can also review if there any available patches for your VM that haven't been installed. As described in the 'Patch installation' previous section, all security and critical updates are automatically installed on your VM using [Automatic VM Guest Patching](#) and no extra actions are required. Patches with other update classifications aren't automatically installed. Instead, they're viewable in the list of available patches under the **Update compliance** tab. You can also view the history of update deployments on your VM through the **Update history**. Update history from the past 30 days is displayed, along with patch installation details.



Updates (Preview) HotpatchCanVM

Assess now Install updates now Manage Configurations Refresh Switch to Update using Automation

Hotpatch status: Enabled [See details](#)

Update compliance Update history

Total missing updates	Missing critical updates	Missing security updates	Other missing updates
2	0	0	2

Last assessed: 2/20/2021 at 10:56

Search by update name... Classifications: All selected

2 items

Update name	Classifications	KB ID	Reboot behavior	Published date
Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1...	Definition	2267602	NeverReboots	2/20/2021, 4:00 PM
2021-02 Cumulative Update Preview for .NET Framework 3.5 and 4.7.2 for Azure Stack ...	Updates	4601557	CanRequestReboot	2/15/2021, 4:00 PM

With automatic VM guest patching, your VM is periodically and automatically assessed for available updates. These periodic assessments ensure that available patches are detected. You can view the results of the assessment on the Updates screen in the previous image, including the time of the last assessment. You can also choose to trigger an on-demand patch assessment for your VM at any time using the 'Assess now' option and review the results after assessment completes.

Similar to on-demand assessment, you can also install patches on-demand for your VM using the 'Install updates now' option. Here you can choose to install all updates under specific patch classifications. You can also specify updates to include or exclude by providing a list of individual knowledge base articles. Patches installed on-demand aren't installed using availability-first principles and may require more reboots and VM downtime for update installation.

You can also view the installed patches using the [Get-HotFix](#) PowerShell command or using the Settings app when using the Desktop Experience.

Rollback support on Hotpatching

The installation of Hotpatch or Baseline updates doesn't support automatic rollback. If a VM experiences an issue during or after an update, you'll have to uninstall the latest update and install the last known good baseline update. You'll need to reboot the VM after rollback.

Next steps

- [Automatic VM Guest Patching](#)
- [Enable Hotpatch for Azure Edition virtual machines built from ISO](#)
- [Azure Update Management](#)