Company Patch Process

The servers located in the datacenter are automatically patched every month using a combination of GPO, WSUS, and Azure Runbooks. Patching is split out by application and environment (Dev, Test, Stage, Production). Generally Dev and Test will be patched early in the month, Stage a week after, and Production the week after that. This allows for problem patches to be caught before being added to Production. The servers in a given Application/Environment are generally patched in Waves, with each wave occurring 30 minutes after the previous wave. This allows for various redundant systems to keep the systems online.

The step-by-step process that patching goes through is laid out below.

# Group Policy

The WSUS group policy is applied at the Organizational Unit level. This policy sets automatic updates to download only, and sets the download location to be the WSUS server.

# Windows Server Update Services (WSUS)

The WSUS server locally stores the needed updates. Updates are then Approved for install to servers. Currently only monthly cumulative updates are approved, and only the previous months updates. This is done to try and stay away from an updates that might cause issues.

# Azure Runbooks

The actual patching itself is controlled by Azure Runbooks, locating in the automation account, in the company subscription.

## Variables

The patch targets are all controlled by Azure variables located in the automation account. In order to add a server to be patched, simply add it to the appropriate variable. Be sure to add the server to both the appropriate All variable, and the Wave variable.

## wsus-checkin Runbook

This runbook runs a script every Sunday/Monday night that forces the targeted servers to check in with the WSUS server and download (NOT install) any needed updates. It uses the various “All” variables to target servers.

## patch-schedule-email Runbook

This runbook runs every morning at 9 AM. It checks upcoming scheduled tasks for patching tasks and then emails appropriate distribution lists warning of upcoming patches. The email includes all the servers that will be patched, what waves are being patched, and when. The emails will be sent out every morning for 3 days prior to patching.

## WSUS-Patch Runbook

This runbook sends the actual commands servers to initiate patch installs. It pulls its target servers from the variable lists mentioned above.