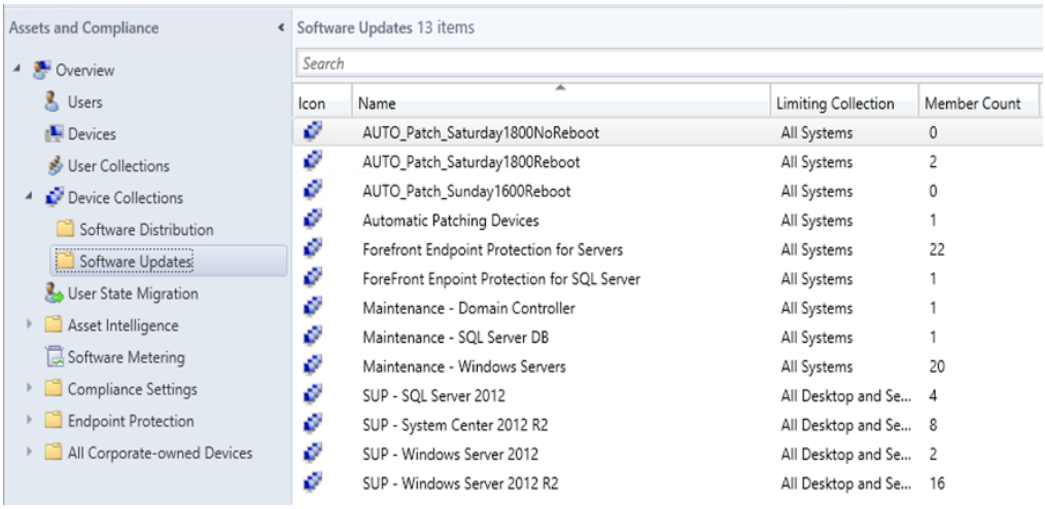
# Kelverion

# Automated Patching Solution

## Automated definition and execution of the monthly patching cycle

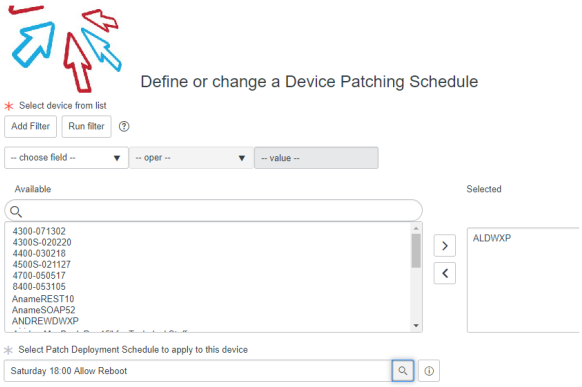
Monthly patch deployments of software and security updates can be a very time consuming and unreliable process, which leaves companies with huge security and compliance issues. When the SCCM Administrator is looking after a large estate or multiple customers, the patching process often becomes a full time job. Many of the same tasks are repeated monthly and the SCCM Administrator becomes the focal point during the process to ensure that devices are patched correctly and working.




A typical set of patching process steps would be as follows:

1. Download the required updates in SCCM
2. Test the updates on some test devices
3. Define and agree with the device owners a schedule for deploying the patches to devices.
4. Create Maintenance Windows so patches deploy at the correct time
5. Raise a Change Request to deploy the patches to the corresponding schedules)
6. Check the deployment collection contains the correct devices for the deployment
7. Create a deployment job per schedule against each collection of devices

The Kelverion Automated Patching Solution is designed to remove this administrative overhead and to increase the flexibility and reliability of the patching process. This is achieved by automating the tasks but also by pushing the ownership of the device patching schedule back to the device owner which increases the control and stability of systems while patches are deployed.




Using this solution the patching process is simply to:

1. Download the required updates in SCCM
2. Test the updates on some test devices
3. Raise a Change Request via the Service Desk portal to deploy the patches

Linking the deployment to a change request it allows greater control of when the SCCM patch deployments are enabled, thus preventing unrequired reboots of critical systems outside of an approved change control window. This is achieved without setting up and maintaining complex maintenance windows in SCCM.

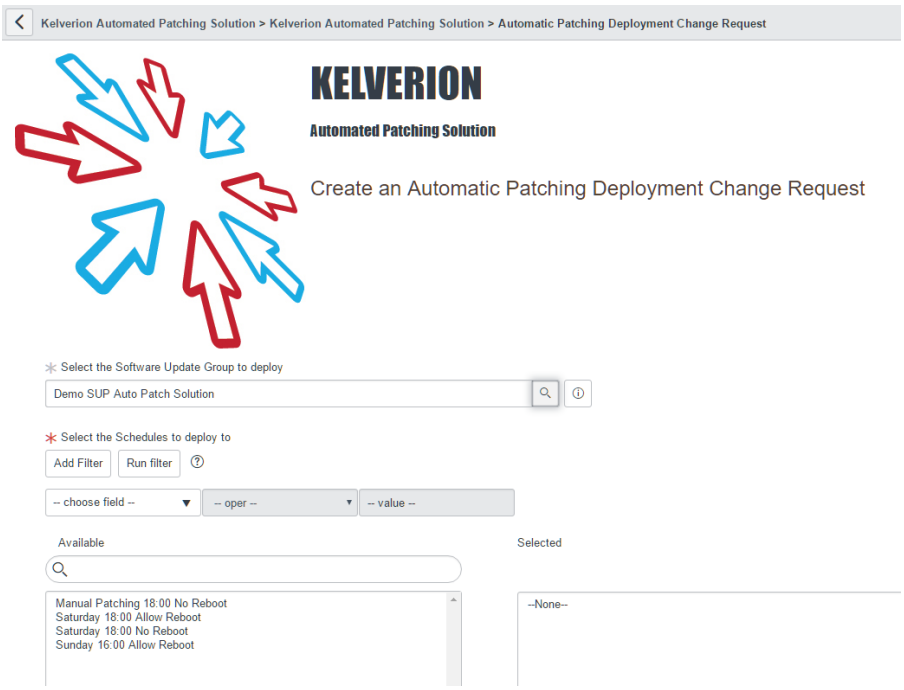
Cloud & Hybrid Automation Experts

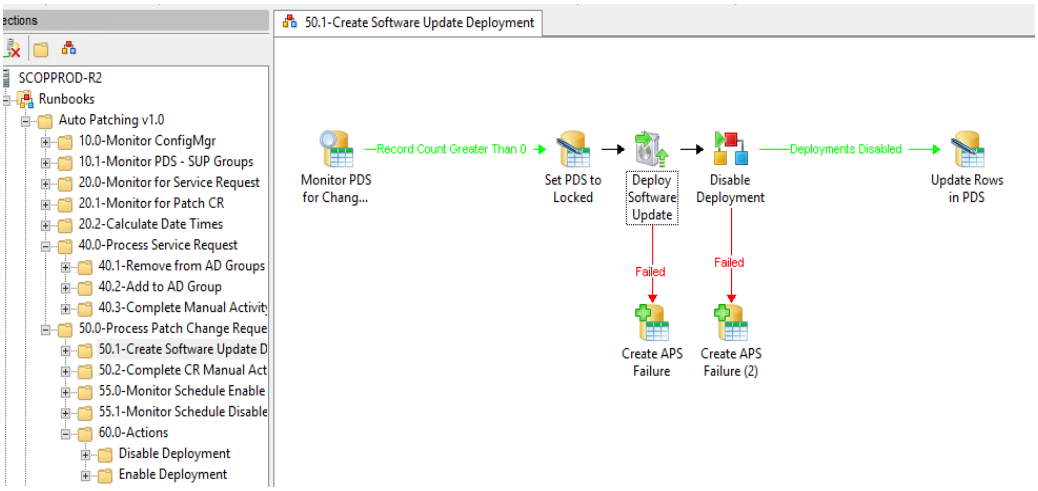
# Kelverion

Device owners define which patch schedule they require for their devices, increasing service availability as this makes it easier to ensure that critical devices don't all patch at the same time taking the service offline. The Patch Schedule selection is controlled via an automated service request from the Service Desk portal.

The use of the Patch Schedule selection also makes it very easy to see which machines should have been manually patched or manually rebooted and then the compliance of those devices can be checked.

The Solution enables SCCM to raise patch deployment failures as SCOM Alerts, so it is immediately obvious which devices require patch remediation.




By leveraging the Test machines as patch masters it becomes easy to use the

Desired State Configuration functionality in SCCM to determine which devices in your estate are not compliant and then SCCM can again raise SCOM Alerts to flag the machine to be resolved.

The usability of the Automated Patching Solution is provided by the Self Service portal capability of the Service Desk. To show the flexibility and reusability of automation solutions, Kelverion provide the Patching Solution with ready built portal components for both ServiceNow and System Center 2012 Service Manager.

The Automated Patching Solution offers a managed approach to control the deployment of software updates and security patches to Windows client devices to increase the patch and security compliancy in the datacenter.

Kelverion are a Microsoft System Center and Cloud Partner who offer Integration Packs and Tools to enhance System Center Orchestrator and Azure Automation and deliver System Center implementation services.
Find out more at http://www.kelverion.com

Cloud & Hybrid Automation Experts