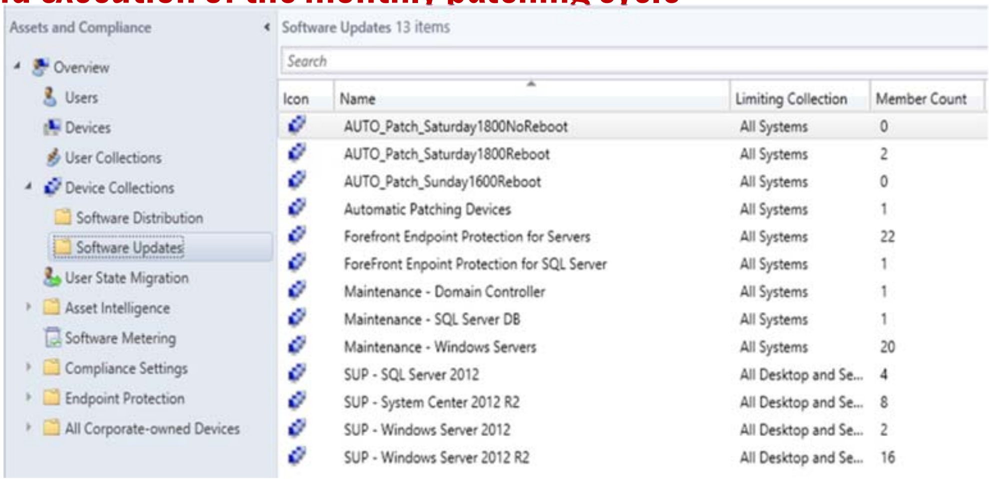
Kelverion

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.

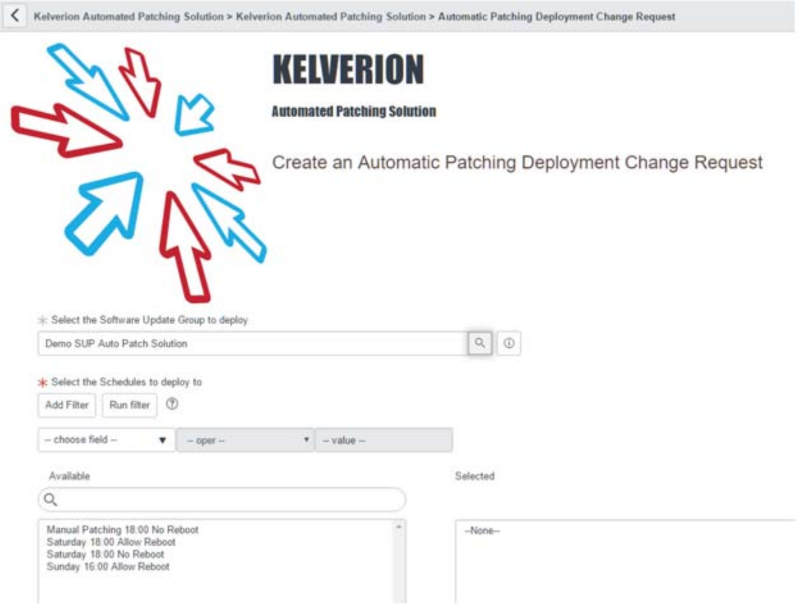


Icon	Name	Limiting Collection	Member Count
	AUTO_Patch_Saturday1800NoReboot	All Systems	0
	AUTO_Patch_Saturday1800Reboot	All Systems	2
	AUTO_Patch_Sunday1600Reboot	All Systems	0
	Automatic Patching Devices	All Systems	1
	Forefront Endpoint Protection for Servers	All Systems	22
	ForeFront Enpoint Protection for SQL Server	All Systems	1
	Maintenance - Domain Controller	All Systems	1
	Maintenance - SQL Server DB	All Systems	1
	Maintenance - Windows Servers	All Systems	20
	SUP - SQL Server 2012	All Desktop and Se...	4
	SUP - System Center 2012 R2	All Desktop and Se...	8
	SUP - Windows Server 2012	All Desktop and Se...	2
	SUP - Windows Server 2012 R2	All Desktop and Se...	16

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.


Kelverion Automated Patching Solution > Kelverion Automated Patching Solution > Automatic Patching Deployment Change Request
KELVERION
Automated Patching Solution

Create an Automatic Patching Deployment Change Request

* Select the Software Update Group to deploy: Demo SUP Auto Patch Solution

* Select the Schedules to deploy to

Add Filter
Run filter
-- choose field --
-- oper --
-- value --

Available:
Manual Patching 18:00 No Reboot
Saturday 18:00 Allow Reboot
Saturday 18:00 No Reboot
Sunday 16:00 Allow Reboot

Selected:
--None--

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.

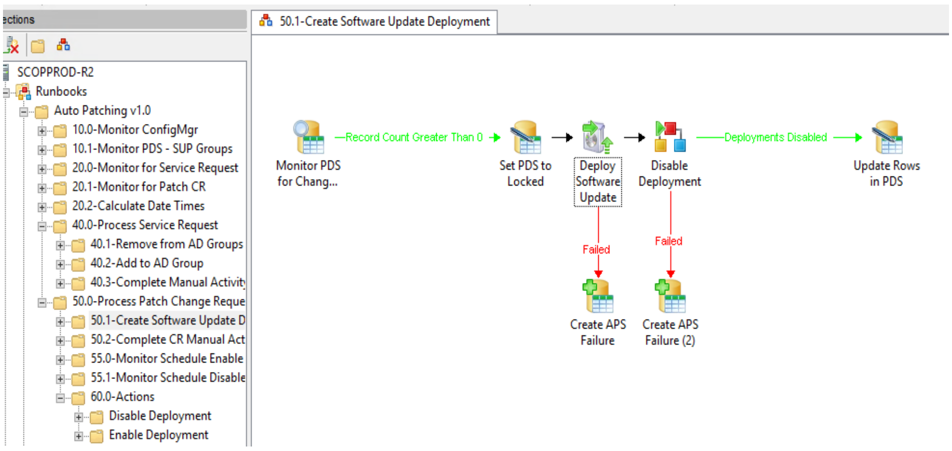
This is achieved without setting up and maintaining complex maintenance windows in SCCM.

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.



ections

- SCOPPROD-R2
  - Runbooks
    - Auto Patching v1.0
      - 10.0-Monitor ConfigMgr
      - 10.1-Monitor PDS - SUP Groups
      - 20.0-Monitor for Service Request
      - 20.1-Monitor for Patch CR
      - 20.2-Calculate Date Times
      - 40.0-Process Service Request
        - 40.1-Remove from AD Groups
        - 40.2-Add to AD Group
        - 40.3-Complete Manual Activity
      - 50.0-Process Patch Change Reque
        - 50.1-Create Software Update D
        - 50.2-Complete CR Manual Act
        - 55.0-Monitor Schedule Enable
        - 55.1-Monitor Schedule Disable
        - 60.0-Actions
          - Disable Deployment
          - Enable Deployment

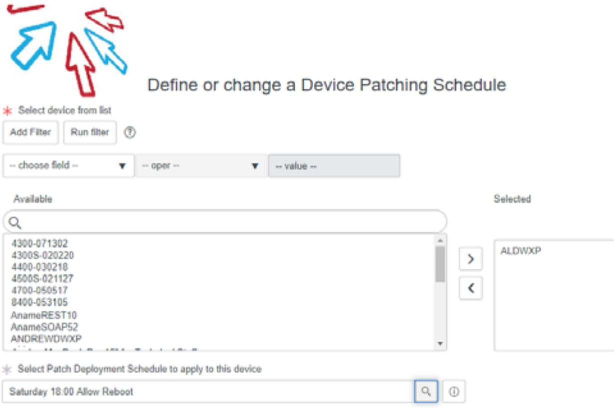
50.1-Create Software Update Deployment

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 the Kelverion Automation Portal.

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.



Define or change a Device Patching Schedule

* Select device from list

Available:
4300-071302
4300S-020220
4400-030218
4500S-021127
4700-050517
8400-053105
AnameREST10
AnameSOAP52
ANDREWDWXP

Selected:
ALDWXP

* Select Patch Deployment Schedule to apply to this device

Saturday 18:00 Allow Reboot

Solution Implementaion

The solution is delivered as a Kelverion lead installation and configuration. In this option you provide Kelverion with remote access to your environment and then a Kelverion consultant will lead the installation and configuration of the solution into your environment and you will provide the subject matter expertise around your Service Desk, SCCM and Active Directory infrastructure configuration.

Up to 40 hours of services delivery is included to deploy the solution.

The implementation hours are valid for 12 months from solution purchase.

Cloud & Hybrid Automation Experts

Scope of the Kelverion led Implementaion

The scope of the Kelverion led implementation is defined as:

1. Integration of solution with ServiceNow only
2. Deployment into a single environment only i.e. Non-Production or Production not both
3. Configuration of the integration to the ServiceNow
4. Configuration of the integration to SCCM
5. An Approved User will enter the ServiceNow Self Service Portal and add devices to a Patch Deployment Schedule thus creating a new Request in the Portal
6. Orchestrator to detect the request and add the Machine to an Active Directory group
7. Orchestrator to then refresh SCCM
8. SCCM Administrator will create a Change Request for deployment of patches to a set of deployment groups
9. Orchestrator to detect the request and create a deployment job within SCCM
10. Orchestrator to enable deployment jobs at scheduled start time
11. Orchestrator to mark Change Request as complete once SCCM instructed to deploy patches

You are responsible for:

- Providing Kelverion with remote access to your environment
- Installing the System Center tools, including Orchestrator and the other target systems
- Creating Collections in SCCM for the Patch Deployment Schedules
- Providing Active Directory Groups which drive membership of the collections
- Downloading and testing patches each month and then creating Software Update Groups in SCCM which are then deployed using the automated process.

Kelverion are an established Independent Software Vendor specialising in IT Automation solutions. Kelverion provides software and specialist consultancy solutions for Microsoft Azure and the Microsoft System Center suite.

Find out more at http://www.kelverion.com

Cloud & Hybrid Automation Experts