The Operations Stack for Vulnerability Management

The Problem

A major multi-national firm with tens of thousands of physical and virtual server instances running hundreds of applications on multiple operating systems and versions across two data centers, multiple in-office labs and server rooms, and multiple public clouds was unable to patch or make security configuration changes across its entire estate. The system administration team relied on SCCM plus AD Group Policy Objects to support multiple versions of Windows-based servers; puppet with shell scripts were used for the Linux servers. On a month-over-month basis, the number of detected vulnerabilities increased by the thousands, despite requiring dozens of labor-intensive over-night and weekend patch windows every month. An emergency patch to address a zero-day vulnerability took over 6 months to be deployed to 100% of servers -- both a significant risk and a compliance violation that had to be disclosed to clients and regulators.

Among the challenges that needed to be addressed were:

- Patch application via SCCM was non-deterministic, once machines were scheduled for | patching then packages were transferred in the background and systems shutdown and rebooted unexpectedly.
- SCCM could not provide information on the real-time state of the patching process. It required accessing the target system to know if a patch had been successfully applied.
- Patching of Linux systems via Puppet covered only a portion of the Linux systems due to distribution differences and provided no error handling or restart capability.
- There was no positive indication if a machine had successfully rebooted.
- System was rate-limited to patching 300 servers (physical or virtual) per shift, with only a 70% success rate.
- There was frequent and significant business impact to failed patching and unscheduled reboots, losing revenue and causing business leaders to demand exempting their critical systems from route patching.

The Solution

There was no single product that could address the vulnerability backlog and keep this increasingly complex server-estate current on patches and security configuration. Careful analysis and lab testing led to the prototype for the Operations Stack for Vulnerability Management, consisting of:

- Centrally managed, network distributed, repositories for operating system and third party patches and in-house application code.
- A distributed, code-driven, cloud-scale orchestration system. The installed topology of the system allowed for patching in multiple highly secured subnets, following mandatory security rules while still allowing for centralized control.

New York ▪ Toronto ▪ Dallas
email: info@opstack.us / tel: 917-916-1006

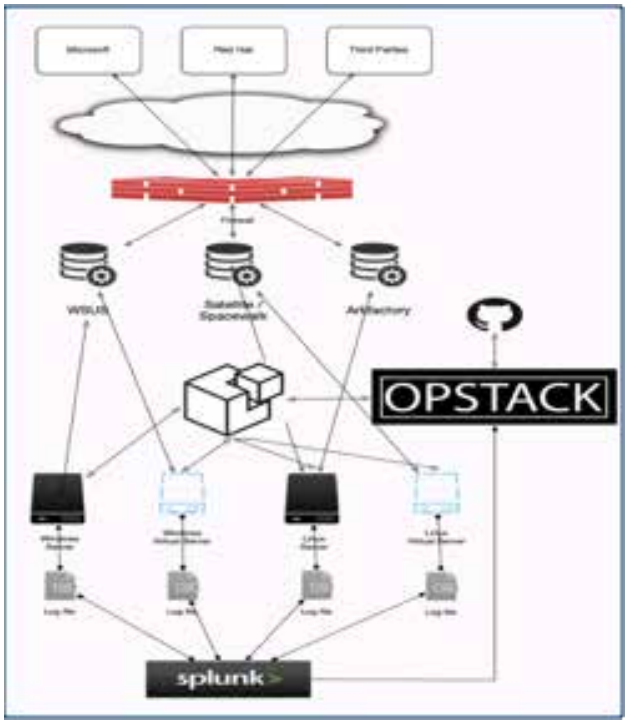
OPSTACK
Thoughtful Operations

- A client agent, written in Python (augmented with PowerShell for Windows servers) that coordinates and logs all patching and configuration activity and provides updates of system state for the CMDB.
- A log aggregation and analytics tool with custom triggers and dashboards to track the progress of patching and configuration changes in near-real-time.

The Result

Once implemented, the results were easily measured -- with many of those metrics coming directly from the stack's log analytics system.

- More than 99.9% of all systems were successfully patched the first time in each run. Real-time information allowed failures to be addressed in minutes, eliminating next-day production downtime
- Patching windows were reduced to 3 per month (non-prod followed two weeks later by two production patching windows scheduled to meet business availability schedules) down from the previous 12.
- Regular patching windows were shortened to under 6 hours (with most completing in 3 hours).
- When faced with emergency patching to address a zero-day vulnerability, tens of thousands of systems were patched in a single overnight patching window.
- The number of engineers required to work overnight shifts to execute supervise patching was reduced by 75%.
- For the first time, the firm could demonstrate compliance with its regulatorily compliant patching policies across its entire on-premise and on-cloud system estate.
- Compliance evidence was generated on a self-service basis from the system, saving multiple person-months of annual effort previously required to provide documentation to regulators and auditors.



New York ▪ Toronto ▪ Dallas
email: info@opstack.us / tel: 917-916-1006

OPSTACK
Thoughtful Operations