SEMI-AUTOMATED SYSTEM UPDATES DEPLOYMENT SOLUTION ASSURING ZERO BUSINESS DISRUPTION

Dimo Bozhidarov Dimov*, Assoc.Prof. Yuliyan Tsonev, Ph.D.**

*Nikola Vaptsarov Naval Academy, Department of Information Technologies, 9026 Varna, Bulgaria, E-mail: dimo.b.dimov@gmail.com

**Nikola Vaptsarov Naval Academy, Department of Information Technologies, 9026 Varna, Bulgaria, E-mail: tzonev@naval-acad.bg

Abstract. Business continuity and availability are top priority for IT. Providing sustainable availability, confidentiality and integrity of all services and resources within associates and counterparts is a key concept to be in the "Leaders" quadrant. Conventionally system updates are being underestimated, delayed or forcefully applied lacking any prior research, analysis nor testing. This paper would glance over an approach providing a flexible and consistent update deployment infrastructure and up-to-date clients, while assuring close to 0 business disruption and having latest critical and security updates in place protecting the organization from current exploits.

Keywords: patches, update, update services, WSUS.

DIGEST

No respectable vendor will reject that systems should be always up-to-date with the latest security patches and fixes available. Having a fully patched environment does not always corresponds very well with the full business automation strategies. From security perspective every reported and proven vulnerability in Microsoft based operating systems and products is addressed in timely manner, removed or fixed. Microsoft experts on updates got a solid approach on defining the problem, the root cause and possible effects on exploiting a certain vulnerability. Monthly and sometimes out-of-band updates are published in order to address vulnerabilities, performance issues and user experience that are directly or indirectly impacting the productivity and/or security of the operating system. Regularly a Security Bulleting is published, reporting details about the updates in the batch, the problems they are addressing and the unlikely event of issues that might appear after the respective patches are deployed.

Most often updates are being ignored, postponed or emergently applied lacking any prior research, analysis nor tests. Any environment is unique having variegated software and application catalog, sophisticated setup and distinctly organized hardware infrastructure. There is no easy way to have up-to-date environment and not to eventually face unexpected failure. There is no single script or rule that would pick and install the proper/needed/important/safe/compatible updates for the different flavors of operating systems (and processor architectures).

The suggested update deployment approach described below could be called semi-automatic. This method of distributing updates combines both – having the newest patches on the systems for the current patching cycle, and having the business undisrupted by keeping the enterprise environment operational.

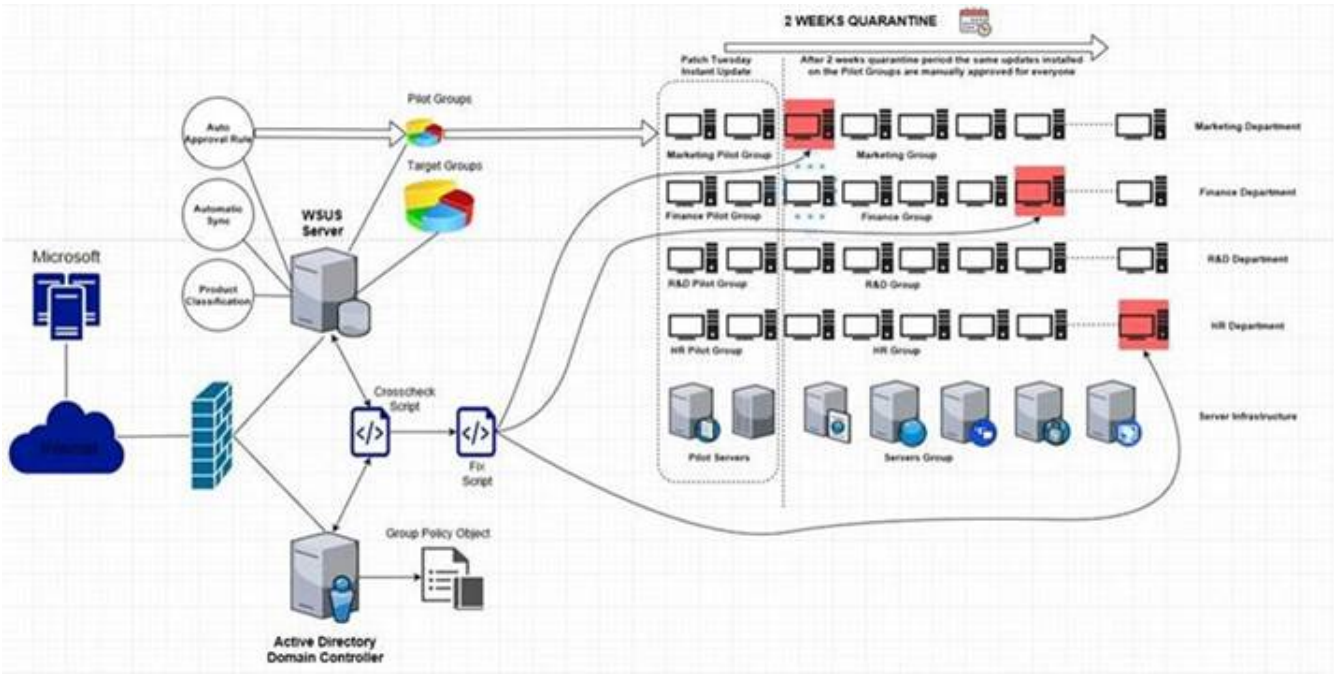
This approach consists of several building blocks (that are defined in more details in the full paper):

1. Windows Server Update Services Server(s) – WSUS Server;
2. WSUS Target groups;
3. Group Policy Objects;
4. Defining Product and Classifications (and Synchronization Schedule);
5. WSUS Automatic Approval Rules;
6. Auto-seek and repair scripts.

On high level, the semi-automatic update deployment is carried out on 3 main stages - ref. Fig. 1:

- WSUS server sync new updates based on the predefined classification and products diversity;
- Newly synchronized updates are immediately automatically approved for the respective pilot groups in the scope of the approval criteria. In case no malfunctions are detected for two weeks 'quarantine' period the process update deployment process continues with next stage;

Figure 1. Semi Auto Update Deployment Concept



- Updates are manually approved for installation to the regular target groups.

Quarantine period may vary depending on the size of the organization, the scope of the tested applications, the number of the OS flavors and the size of pilot groups. However, 2 weeks period is a reasonable time for both – testing the newest updates (performed on pilot groups) and postponing the delivery of the same updates (for the rest of the clients of the WSUS infrastructure).

Extremely important topic is to have near to 100% coverage of the updates on the hosts so it is vital to understand the actual percentage of clients that are reporting back and synchronizing updates with WSUS. There might be multiple reasons for failure but applying auto-search and fix scripts has shown tremendous results on searching for missing clients and attempting to restore the communication between them and WSUS server (scripts are included in the full paper).

In case out-of-band updates are released and are addressing significant vulnerabilities with critical severity in terms of security, the patching cycle (test-quarantine-deployment) could be skipped. Ad-hoc emergency testing team containing critical business processes involved departments should be organized. Testing team should consist of department champions and would be tasked with emergency application test during and after the update installation. In case no issues are detected – critical updates are to be urgently mass deployed.

Security is a must. Having a secured environment means having up-to-date environment.. Underestimating or excessively delaying the updates of any piece of the corporate infrastructure – servers, storage, workstations, mobile devices (smartphones, tablets), network equipment (OS and

firmware), will eventually cause devastating results on the business processes and company reputation. Blindly trusting any newly released updates on the other hand, and applying without prior testing and analysis could potentially damage a decently working setup. Proper scaling and fine tuning a Windows Update Infrastructure would deliver the needed updates in a timely manner. It will assure more secure environment along with the compatibility and business continuity by having the supplied updates, patches and service packs.

REFERENCES

[1] https://technet.microsoft.com/pt-br/library/cc720448(v=ws.10).aspx
[2] https://msdn.microsoft.com/en-us/library/windows/desktop/ms744629(v=vs.85).aspx
[3] https://www.information-management.com/news/business-continuity-and-availability-remains-top-priority-for-it?_ga=2.241559877.670405502.1518508041-1748625795.1518508041
[4] https://blog.athoc.com/athoc-blog/241-5-reasons-business-continuity-is-a-top-priority-for-it-departments.html