ADAPTIVE PATCHING STRATEGY

PhD. Student Dimo Bozhidarov Dimov[x], Assoc. Prof. Yuliyan Tsonev[y]

Nikola Vaptsarov Naval Academy, Bulgaria[xy]

ABSTRACT

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. No respectable vendor will reject the idea that systems should be always up-to-date with the latest security patches and fixes available. Having a fully patched environment does not always correspond very well with the full business automation strategies. This article glances over an approach for delivering latest updates to Microsoft systems and at the same time putting minimum degradation of the production systems process.

Keywords: *patching, updates, group policy object, WSUS.*

1. INTRODUCTION

Business continuity and availability remains top priority for IT as per survey amongst 5632 worldwide IT professionals [3]. Continuity = security: continuity and security are symbiotic, and the health of one greatly impacts the other. Responsible IT leaders understand their role within the context of the larger organization [4]. 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.

The following article will 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. 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.

Digested this patching strategy consist of several building blocks.

2. WINDOWS SERVER UPDATE SERVICES SERVER(S) - WSUS SERVER

Proper designing, scaling and implementing the Microsoft Update deployment infrastructure is of critical importance for any company, enterprise or organization that wants to run stuff by the book. In order for all the clients to receive critical and/or security updates properly and on time first a scope of the environment should be defined.

The most basic WSUS deployment consists of a server inside the corporate firewall that serves client computers on a private intranet, as shown in the "Simple WSUS Deployment" illustration on Figure 1. The WSUS server connects to Microsoft Update to download updates. [1]

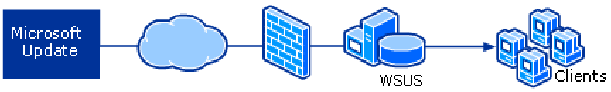


Figure 1. WSUS deployment with a single WSUS server

If all the infrastructure is situated in a single office then a single WSUS server should be sufficient if many major locations are to be targeted, containing many clients then line speed and line availability between those locations should be considered as well as the exact number of the targeted clients. In case a large infrastructure should be designed to cover the proper patching of a significant number of clients spread geographically, then downstream servers should be included in the implementation – Figure 2.

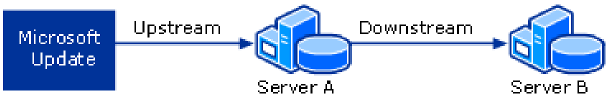


Figure 2. WSUS deployment with multiple WSUS servers.

Using multiple WSUS servers allows you to scale WSUS in a large organization. If the organization uses multiple WSUS servers, one of the servers will act as the upstream WSUS server (the remaining servers are downstream servers). You use the upstream server to specify the updates that you want to synchronize with Microsoft Update. [2]

Large infrastructures should have a strict and simple design (whenever possible) and best case is to be centrally administrated. Central administration should cost less and will have the environment consistent in terms of configuration and content. Such setup could be achieved by taking advantage of replica downstream servers.

A replica downstream server replicates the upstream server. The replica server synchronizes the same updates as the upstream server, and has the same target groups, approvals, accepted license agreements (EULAs), and declined status as the upstream server. The only difference between an upstream server and the replica server is the clients that are assigned to the target groups. [2].

3. WSUS TARGET GROUPS

WSUS allows to target updates to specific target groups. Those groups are not Active Directory groups, but WSUS specific groups. Clients (workstations and servers) could be directed into their respective group by 2 means – using server-side or client-side targeting. By default, when any client 'meet' the WSUS server for the first time is moved into the default group. Afterwards they could be moved manually by WSUS console (using the server-side method) or by client-side – setting pushed by a GPO (group policy object). Since we are seeking automation (whenever safe) the method that will be utilized is client-side targeting and will be a subject of a consecutive building block.

It is recommended to segment, to group the clients that will be receiving updates. This segmentation should be based on certain organization specific criteria. Clients could be grouped by geographical location (city or country where they are located). Smart way for the clients to be grouped is by the role they are assigned in their organization – devices in the financial department are moved to "Financial Group", marketing department devices are in "Marketing Group", devices in R&D department in "Research and Development Group". Similar segmentation would provide great flexibility in terms of approving different updates and fixes on diverse groups. Different departments are utilizing various applications – financial, graphical, development, etc. and so are having various types of setups. Assuring 100% compatibility among the corporate application catalog and the newly published patches could be tough and challenging endeavor.

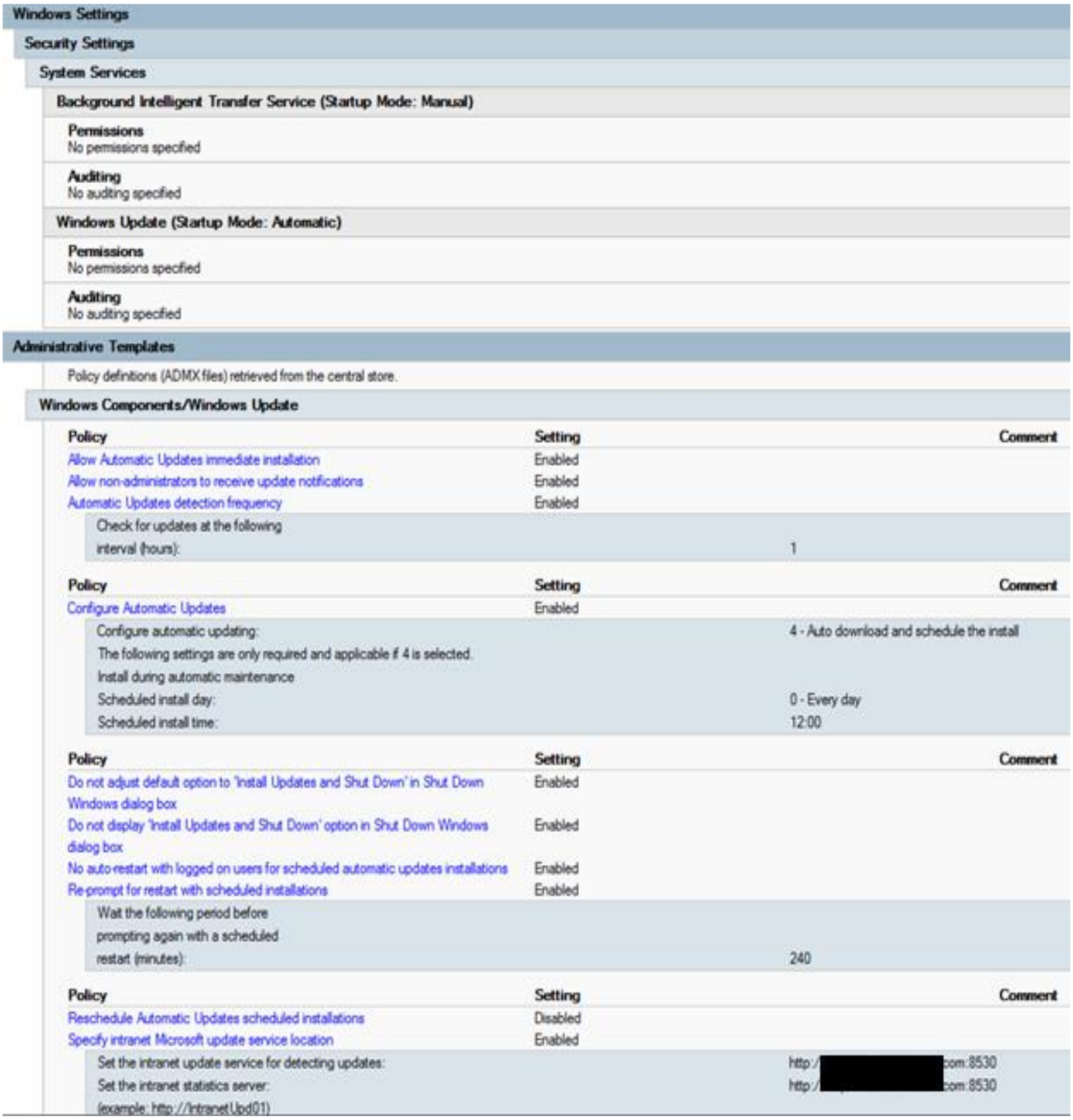
It is not an unlikely event for a newly deployed update to crash a certain application(s) and/or driver(s) to stop operating properly. Sporadic hangs of any apps or the entire OS itself can occur upon installation of the newest patches. Updates publishers and developers are usually quickly addressing such events by providing updated versions of the patches, brand new patches and hotfixes. Having your system not up-to-date is inevitably exposing critical vulnerabilities that could be exploited by a well-prepared attacker. On the other hand, impetuous implementations of this-morning released updates on productive systems without prior testing and analysis will sooner or later bring performance degradation, business disruption or entire system outage. Crucial necessity of immediate installation of security related updates (for OS or applications) must be well calculated and balanced in order for any negative results to be avoided. Administrators strive to keep current systems updated. There are many threads related to handling auto approval – a method where the administrator prepares rules, based on which updates having certain classification and/or severity, are approved for installation on specific groups. Any automations are beneficial from an IT perspective. However, automation is not always providing the agility needed by the business.

Besides production, IT advanced organizations should maintain also a testing and a quality environment. But let's be honest. What is the number of organizations that are actually managing consistent test, quality and production environments and are maintaining the change management by the book? The suggested strategy would need pilot groups. Those pilot groups should contain client representatives, sample of the previously segmented groups. The purpose of the pilot groups is for them to be the first receivers of the newest published updates. In case something goes horribly wrong, the rest of the organizational infrastructure will remain intact by not receiving the problematic/incompatible patches. It is easy for an IT guy to check, test and deploy a software update. But the IT guy cannot have all the knowledge for the functionalities that all the users in the organizations are utilizing within the corporate applications. Furthermore, a true valid test must be performed with live users. Along with the creation of "Financial Group", "Marketing Group", "Research and Development Group" similar pilot groups will be created: "Financial Pilot Group", "Marketing Pilot Group", "Research and Development Pilot Group".

In best case the piloting users will be working on business-critical processes and applications across the company and are having more advanced IT skills. These personnel should be advised and encouraged to look for any unexpected, problematic or abnormal behavior not only for their dedicated applications but for the entire OS itself. The nominated pilot users will be acting as live testers. Piloting time phase should be long enough for the pilot users to be able to monitor the behavior of the systems during and after patching, and short enough so the environment will not be deprived from the newest updates.

4. GROUP POLICY OBJECTS

WSUS clients could be either workstations or servers. The WSUS clients should be 'forwarded' to their WSUS server and their respective target group. Usually this is done by a Group Policy Objects (GPOs) applied on the respective objects. The group policy object setting on Figure 3 specifies a certain setting, configurations and values needed by the client in order to seamlessly connect, synchronize, download, install, reboot (if needed) and complete the deployment of the patches.



Windows Settings

Security Settings

System Services

Background Intelligent Transfer Service (Startup Mode: Manual)

Permissions
No permissions specified

Auditing
No auditing specified

Windows Update (Startup Mode: Automatic)

Permissions
No permissions specified

Auditing
No auditing specified

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

Windows Components/Windows Update

Policy	Setting	Comment
Allow Automatic Updates immediate installation	Enabled	
Allow non-administrators to receive update notifications	Enabled	
Automatic Updates detection frequency	Enabled	
Check for updates at the following interval (hours):	1	

Policy	Setting	Comment
Configure Automatic Updates	Enabled	
Configure automatic updating:	4 - Auto download and schedule the install	
The following settings are only required and applicable if 4 is selected.		
Install during automatic maintenance		
Scheduled install day:	0 - Every day	
Scheduled install time:	12:00	

Policy	Setting	Comment
Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box	Enabled	
Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box	Enabled	
No auto-restart with logged on users for scheduled automatic updates installations	Enabled	
Re-prompt for restart with scheduled installations	Enabled	
Wait the following period before prompting again with a scheduled restart (minutes):	240	

Policy	Setting	Comment
Reschedule Automatic Updates scheduled installations	Disabled	
Specify intranet Microsoft update service location	Enabled	
Set the intranet update service for detecting updates:	http:/[redacted]com:8530	
Set the intranet statistics server:	http:/[redacted]com:8530	
(example: http://IntranetUpd01)		

Figure 3. Sample of GPO setting related to maintaining updates

Some of the main settings that are reasonable to be deployed via GPO are the following:

-Windows Update Service – Startup Mode: Automatic. Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API;

-Automatically check for updates every hour. This policy specifies the hours that Windows will use to determine how long to wait before checking for available updates. The exact wait time is determined by using the hours specified here, minus 0~20% of the hours specified;

-In case a new update is available – the client will download and schedule the update for installation. In this specific case updates are installed daily at 12 o’clock;

-No auto-restart with logged on users for scheduled automatic updates installations - prevents automatic restart when a user is signed in. If a user schedules the restart in the update notification, the device will restart at the time the user specifies even if a user is signed in at the time;

-Reschedule automatic updates scheduled installation – Disabled;

-Defining WSUS server and port where clients should connect to synchronize;

-Defining WSUS server and port where statistics data to be collected;

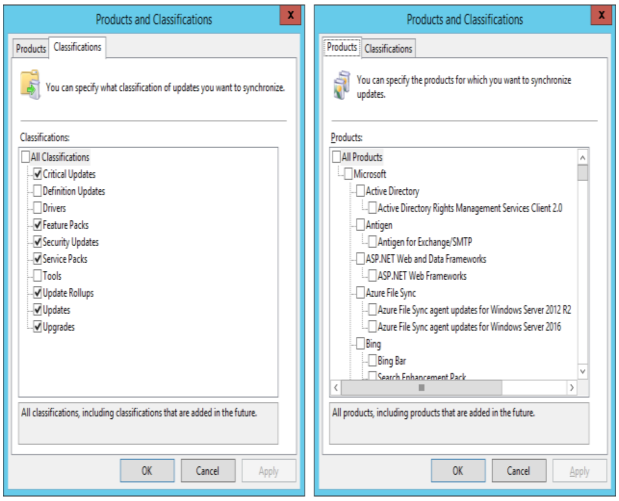
-Target group name for this computer – Specifies the target group name or names that should be used to receive updates from an intranet Microsoft update service;

-The specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed.

If the GPO does not specify a certain group where the respective client should be moved to – the client is placed to a default group.

5. DEFINING PRODUCT AND CLASSIFICATIONS (AND SYNCHRONIZATION SCHEDULE)

By utilizing this functionality, we could specify the product for which we would like to receive updates and what type of updates we would like to be downloaded to the WSUS server.



Products and Classifications

Products | Classifications

You can specify what classification of updates you want to synchronize.

Classifications:

- □ All Classifications
  - ☑ Critical Updates
  - □ Definition Updates
  - □ Drivers
  - ☑ Feature Packs
  - ☑ Security Updates
  - ☑ Service Packs
  - □ Tools
  - ☑ Update Rollups
  - ☑ Updates
  - ☑ Upgrades

All classifications, including classifications that are added in the future.

Products and Classifications

Products | Classifications

You can specify the products for which you want to synchronize updates.

Products:

- □ All Products
  - □ Microsoft
    - □ Active Directory
      - □ Active Directory Rights Management Services Client 2.0
    - □ Antigen
      - □ Antigen for Exchange/SMTP
    - □ ASP.NET Web and Data Frameworks
      - □ ASP.NET Web Frameworks
    - □ Azure File Sync
      - □ Azure File Sync agent updates for Windows Server 2012 R2
      - □ Azure File Sync agent updates for Windows Server 2016
    - □ Bing
      - □ Bing Bar
      - □ Search Enhancement Pack

All products, including products that are added in the future.

Figure 4. Example of Update Classification and Products available.

Of course, bringing a piece of automation will ease the administration by scheduling an automatic synchronization between the WSUS server and Microsoft - for example once a day.

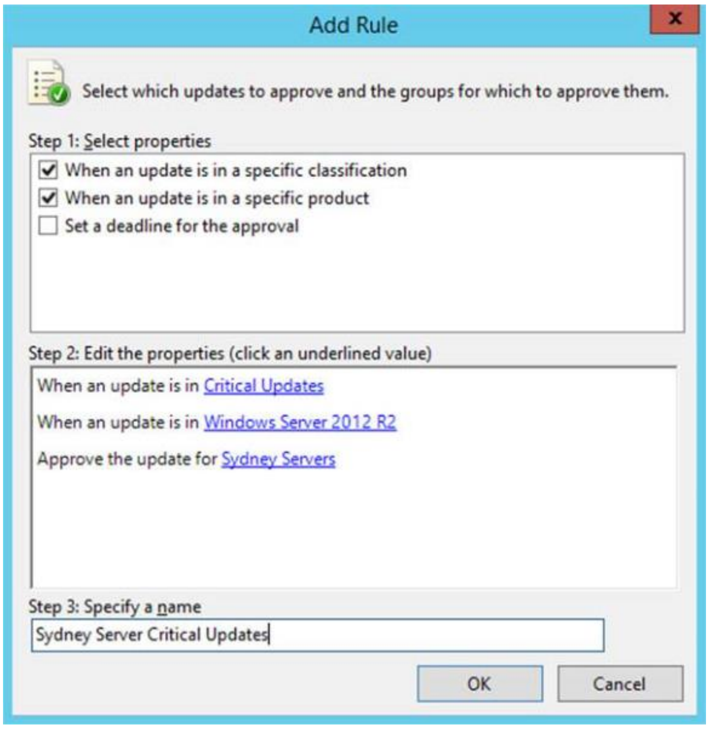
Defining the Product and Classifications is based on the following criteria: Product - OS version and/or flavor, Office, Active directory, Internet Explorer, etc.; Classification - critical updates, definition updates, drivers…; Ref. Figure 4.

After products and update classifications are selected, WSUS server is ready to be synchronized. The synchronization process involves downloading updates from Microsoft Update or another WSUS server. WSUS determines if any new updates have been made available since the last synchronization. The initial synchronization on a WSUS server will take considerate amount of time. No changes will be available on the server's update filters (products, classifications, languages) while the server is synchronizing.

6. WSUS AUTOMATIC APPROVAL RULES

Current building block is related to the automatic approval of specifically selected updates. The approval rule has two major critical aspects – the criteria by which the updates are selected (filtered) and which group(s) the selected updates will be applied to. Automatic approval rule should be created in WSUS environment based on carefully selected criteria. Similarly, to the previous topic, those criteria could include: classification (critical updates, definition updates, drivers…), product (OS version, Microsoft product…), and deadline.

The WSUS environment allows for the approval rules to be extremely fine-tuned and adjusted so no unexpected updates will be delivered for the group that the rule is applied on. Far from recommended is to compile heavy rules, containing various types of OS, products and severity ratings. More flexible approach is to create multiple fine-grained rules that are easier to combine in a manner to deliver the targeted results.



Add Rule

Select which updates to approve and the groups for which to approve them.

Step 1: Select properties

☑ When an update is in a specific classification
☑ When an update is in a specific product
□ Set a deadline for the approval

Step 2: Edit the properties (click an underlined value)

When an update is in Critical Updates

When an update is in Windows Server 2012 R2

Approve the update for Sydney Servers

Step 3: Specify a name

Sydney Server Critical Updates

Figure 5. Approval Rule Example

Once defined, the outcome is a self-explanatory screen providing all the information related to the rule needed by the administrator – ref Figure 5.

7. AUTO-SEEK AND REPAIR SCRIPSTS

This last building block is not mandatory at all. Still it is included in the overall approach aiming to deliver holistic response experience even for the most challenging expectations. Extremely important topic is to have near to 100% coverage on the hosts so it is of great importance to understand the actual percentage of clients that are reporting back and synchronizing updates with WSUS. There are always clients that are not reporting to WSUS for some reason. It is up to the update administrator to track down such clients and force them to report. There might be multiple reasons for failure but the following technique has shown tremendous results on searching for missing clients and attempting to restore the communication between them and WSUS server.

The technique consists of 2 relatively simple steps:

1. A script runs a crosscheck between Active Directory database and WSUS database to find any discrepancies – computer objects existing in AD DB but missing in WSUS DB;
2. The reported discrepancies (computer objects) are targeted one by one with another script attempting to fix the

communication between the client and WSUS.

On high level the PowerShell script below takes all the clients in WSUS on one side, takes all computer objects that are online and have Time Stamp from the last 60 days and generates a list. This list contains online objects existing in AD, but missing in WSUS. Those clients that are operational in AD but are not reporting to WSUS are passed to PSExec tool which run another script targeting one by one on all the outcasts.

```
Get-Date

Get-Process | where {$_.Name -eq "psexec"}
| Stop-Process -Force -Verbose

$pclist = @()
$wsuslist = Get-WsusComputer -All | select
FullDomainName

Get-ADComputer -Filter * -SearchBase
"DC=mydomain,DC=com" -Properties
Name,DistinguishedName,LastLogonTimestamp
|
select
Name,DistinguishedName,@{n='LastLogonT';e=
{[DateTime]::FromFileTime($_.LastLogonTime
stamp)}} |
where { ($_.DistinguishedName -like
"*workstation")`
 -and $_.LastLogonT -gt ((Get-
Date).AddDays(-60))} | select Name |
ForEach-Object{
    $hostlookup = $_.Name + "*"
    if ($wsuslist.FullDomainName -like
$hostlookup)
    {
    }
    else
    {
        $pclist += $_.Name
    }
}

Write-Host "Targeted Hosts"
$pclist

Write-Host "Online hosts"

$pclist | ForEach-Object {
    $psargument = "\\" + $_ + " -s
\\mydomain\netlogon\scripts\WSUS_Reset.bat
"
    if (Test-Connection -ComputerName $_ -
Quiet -Count 1)
    {
    Write-Output $psargument
    Start-Process -FilePath
"\\mydomain\netlogon\PSTools\psexec.exe" -
ArgumentList $psargument -
RedirectStandardError
"C:\Scripts\psexecerror.log"
    Start-Sleep -Seconds 10
    }
}
```

The second script is simpler and it runs locally on the problematic host. The script stops the update service on the client computer. Deletes some registry keys. Deletes the update services data store database. Start the update services on the computer and forces the client to look for updates.

Keys /reset authorization /detect now are resetting the cookie that is used by the process. If there are changes in the configuration of the server, for example by setting up group targeting, then this will ensure that the latest settings are used.

```
net stop wuauserv
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\WindowsUpdate /v PingID /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\WindowsUpdate /v AccountDomainSid /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\WindowsUpdate /v SusClientId /f
reg Delete
HKLM\SOFTWARE\Microsoft\Windows\CurrentVer
sion\WindowsUpdate /v
SusClientIDValidation /f
del /F /Q
c:\Windows\SoftwareDistribution\DataStore\
datastore.edb
net start wuauserv
wuauclt.exe /resetauthorization /detectnow
```

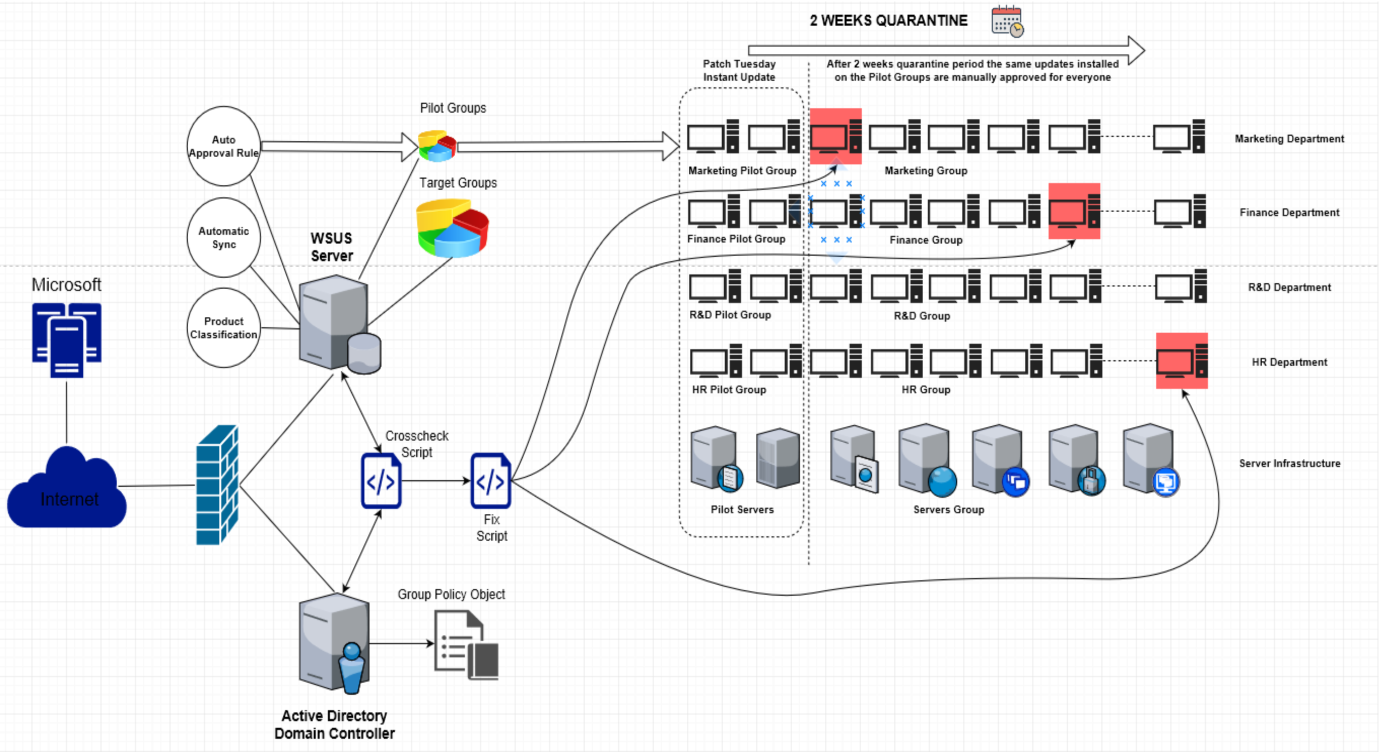


Figure 6. Adaptive Patching Concept

After collecting all the pieces of the picture: WSUS server(s); group policy objects setting WSUS configs and directing clients to their respective WSUS group; pilot group segmentation in WSUS environment; defining products and classifications of the updates that are downloaded from Microsoft; automatic approval rules; automatic synchronization; – the system is ready to go live. Depending on the size of the updates and the scale of the infrastructure the whole patching process time may vary significantly.

On high level, the adaptive patching deployment is carried out on 3 main stages:

1. WSUS server sync new updates based on the predefined classification and products diversity;
2. 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 by manually triggering stage 3;
3. 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).

8. CONCLUSIONS

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.

9. 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