WSUS
Architektura, nastavení a nasazení

Ing. Bohuslav Frk, MCSA

WSUS – Co to je a co přináší

- WSUS je lokální Windows update

Přináší
- Jednoduchou možnost společné instalace a konfigurace aktualizací
- Přehled o nainstalovaných aktualizacích v síti (lze kombinovat s MBSA)
- Výrazná úspora přenosové kapacity internetové konektivity

Lze použít na
Od Windows 2000 výše

Nezapomeňte na CRL Types for SQL a Report Viewer

Doporučení nedávat data ani databázi na systémový disk

WSUS Instalace

Na W2008 a výše je to role.

Kroky při instalaci lze následně měnit v konfiguraci již nainstalovaného WSUS.

Některé ale složitě (port v IIS, SQL databáze), jiné velmi složitě (umístění aktualizací) = Je důležité mít již při instalaci vše rozmyšleno.

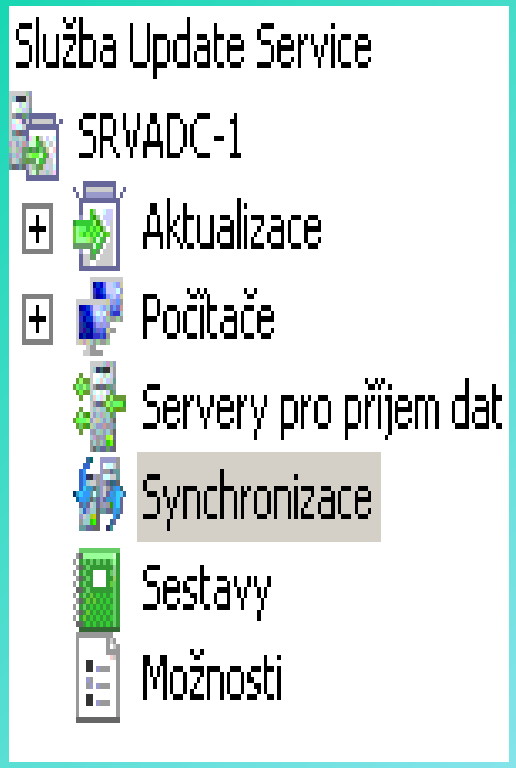
Pokud se v instalaci nezaškrtne a nevyplní umístění aktualizací místně, bude se pouze řídit schvalování, ale počítače si to budou stahovat z Windows Update

Po instalaci je nutné provést první synchronizaci, pro načtení všech dostupných produktů.

Správa přes MMC3 (Pro WSUS 2.0 byla správa přes IE)

Pro konzoli je minimální požadavek Win XP SP2. Instalace ne přes RSAT ale přes instalační soubor WSUS a vybrat pouze konzoli.

WSUS – Používání



Aktualizace - Přehledy, vlastní pohledy, filtrování a odsouhlasování aktualizací. Vetšinou vystačíme s pohledem **Všechny aktualizace** a fitrem **Neschvalená** a **Selhala nebo potřebná.**

Počítače – Vytváření skupin, Vlastní pohledy nejdou. Většinou si vystačíme s pohledem **Všechny počítače** a fitrem **Selhala nebo potřebná.**

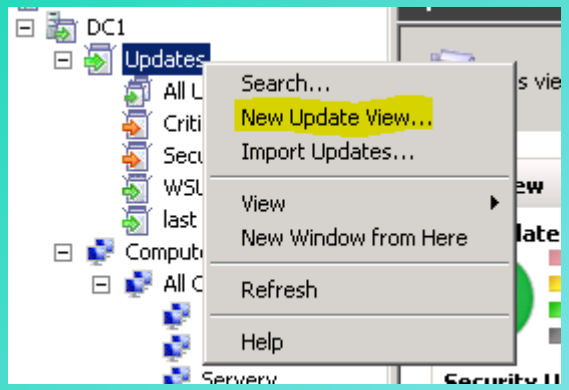
Synchronizace – stejný report jako v sestavách. Dostupnost logů tři měsíce.

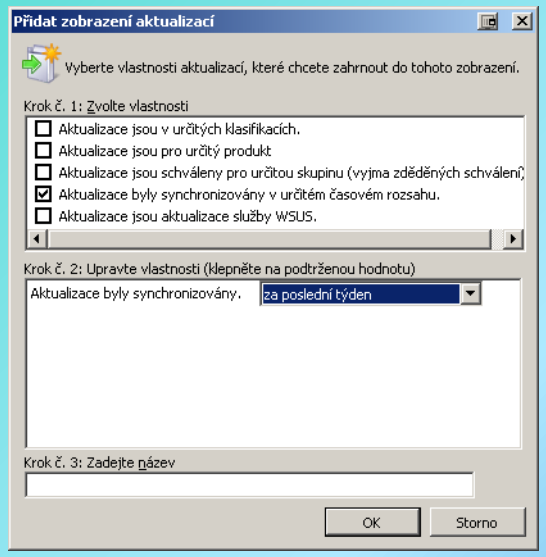
Sestavy **–** možnost generování sestav pro aktualizace, počítače a synchronizace.

Možnosti – Vlastní nastavení WSUS serveru.

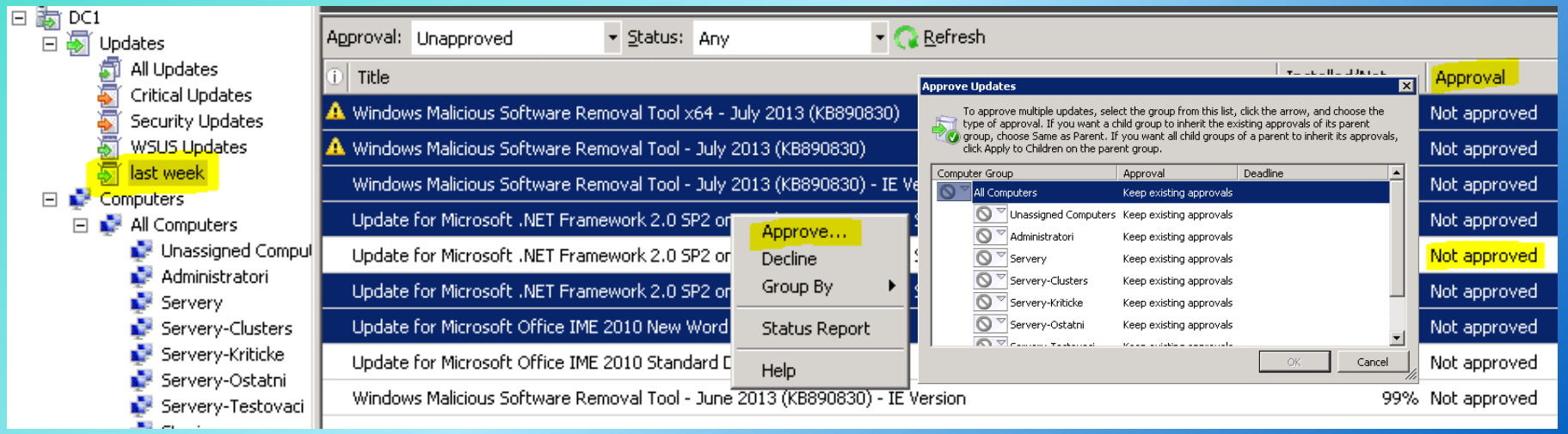
WSUS updaty

WSUS server automaticky nebo ručně stáhne updaty
Updaty vidíme v přehledu „updates“ a kromě defaultních zobrazení můžeme používat vlastní:



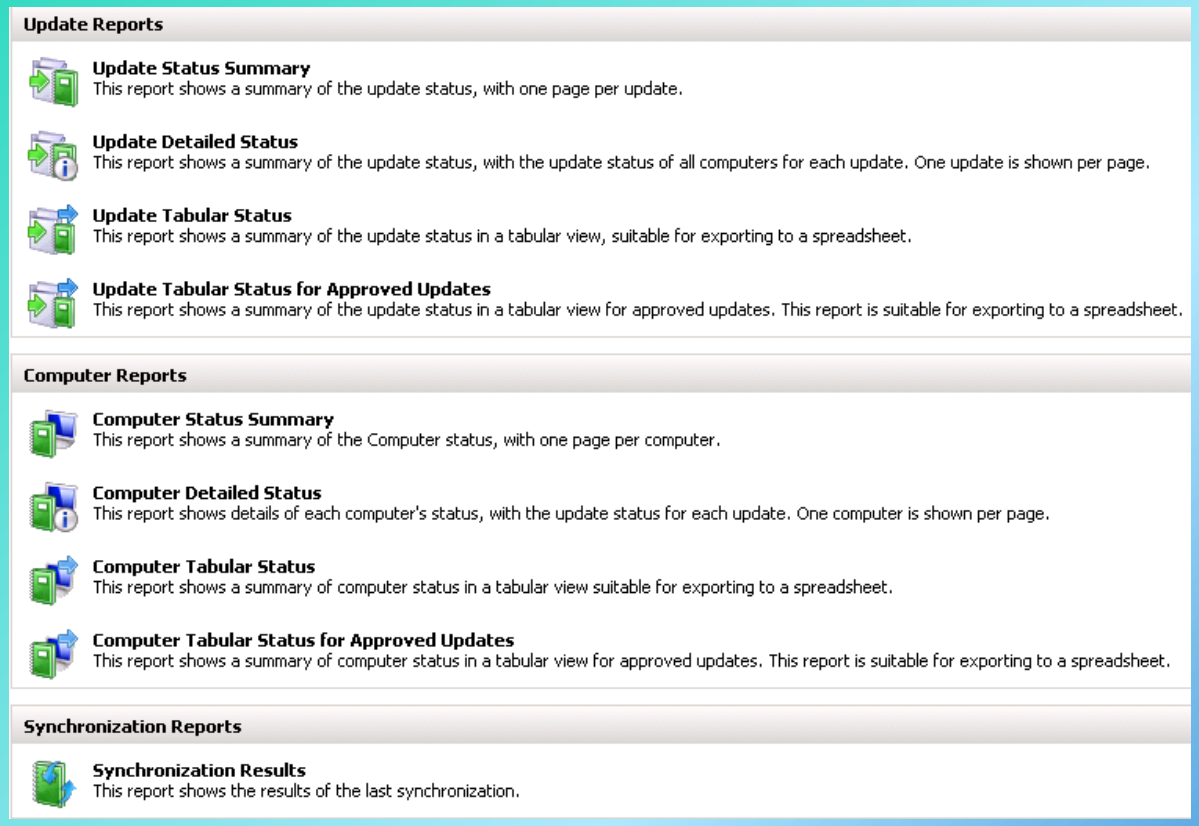


S použitím default nebo custom view následně schvalujeme updaty k distribuci:



WSUS Reporty

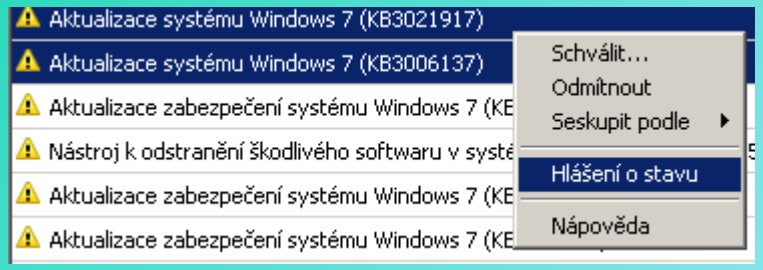
WSUS disponuje možností reportů pro detailní přehled o statusu updatů a počítačů



Pro jistotu a ověření můžeme také stroje na síti oskenovat pomocí např.: MBSA

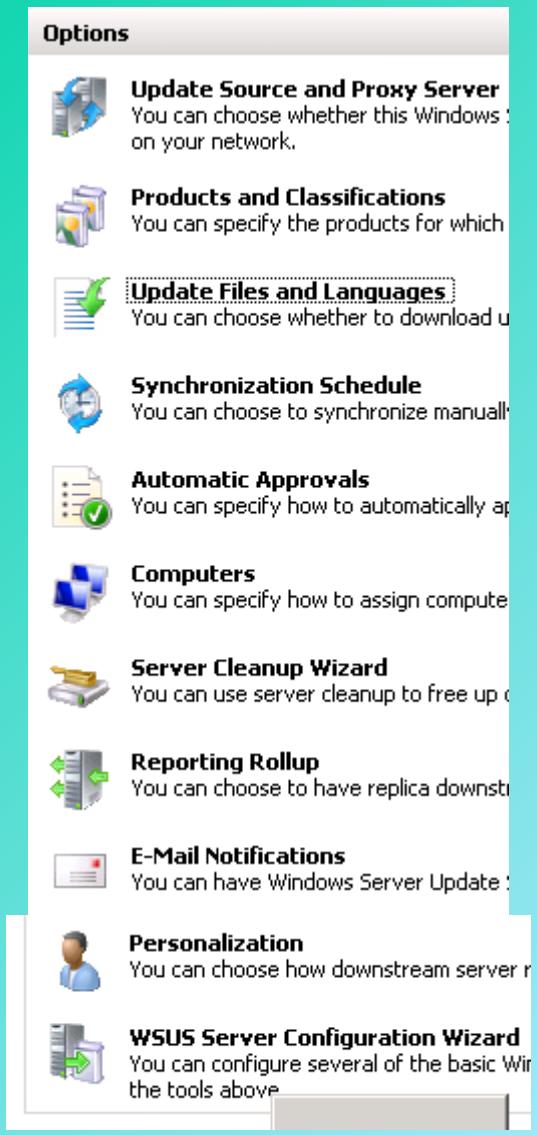
Sestavy

Sestavy lze generovat i nad vybranými počítači nebo aktualizacemi (pravé tl. – hlášení o stavu)



Na symbolu diskety lze uložit jako Excel, Word nebo PDF

WSUS OPTIONS



Nastavení :

- Všechna podstatné nastavení jsou zde
- Co se bude stahovat
- Jak se to bude stahovat
- Co se bude samo schvalovat
- Odkud se to bude stahovat
- Kdy se to bude stahovat
- Způsob distribuce
- Údržba serveru
- Mail notifikace

Toto se zpravidla nastaví jen jednou a potom server udržujeme hlavně z pohledu schvalovaní, kontroly průběhu patch managementu.

WSUS – Nastavení serveru

Zdroj aktualizací a proxy server

Možnost stahovat z upstreamu nebo ze serveru Microsoftu

Porodukty a klasifikace

Všechny produktu dostupné až po prvotní synchronizaci

Rozmyslet si instalaci Service Packů

Jazyky a soubory aktualizací

- *Soubory rychlé instalace*. Zvýší se stahování z Microsoftu, sníží se tok mezi WSUS a klienty. WSUS porovná soubory s už nainstalovanými na stanicích a pošle jenom rozdílné Byty (Delta přenos). Používá se u větších sítí nebo pomalou LAN (WAN) - default je vypnuto. Vetší přenos z MS je způsoben stahováním všech variant souboru k aktualizaci.

- Vždy vybrat pouze konkrétní jazyky.

Plán synchronizace

Zadává se prvotní čas a pak číslo kolikrát denně (24 hodin se dělí následně na tyto intervaly s daným počátkem první synchronizace). Stáhnou se pouze metadata pro detekci aktualizací.

Automatické schvalování

Možnost vytvořit pravidla schvalování. Mělo by se používat velice obezřetně na testovací počítače.

Počítače

Možnost výběru zařazování přes Group policy, nebo ručně z konzole WSUS

Průvodce vyčištěním serveru

Průběžně čistit server. Vyhneme se tak zbytečnému zaplnění databáze a filesystému

Souhrn hlášení

Možnost definovat typy reportů ze WSUS

WSUS – Nastavení serveru

Emailová upozornění

Definice upozornění serveru WSUS na nové aktualizace a stavy počítačů.

Přizpůsobení

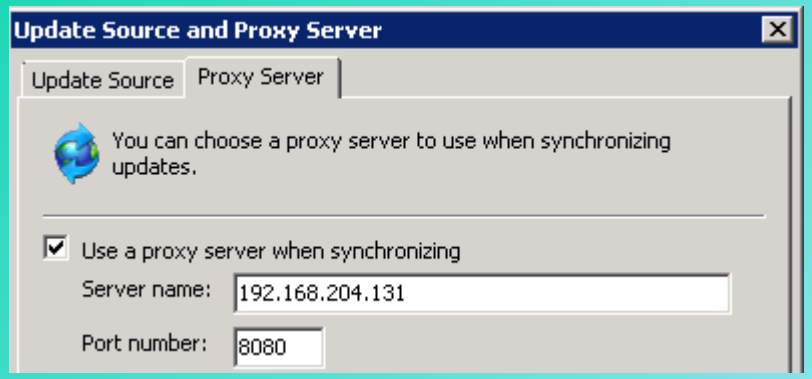
Nastavení příjmu stavů z replik
Nastavení úkolů pro zobrazení na úvodní obrazovce konzole WSUS

Průvodce konfigurací serveru služby WSUS

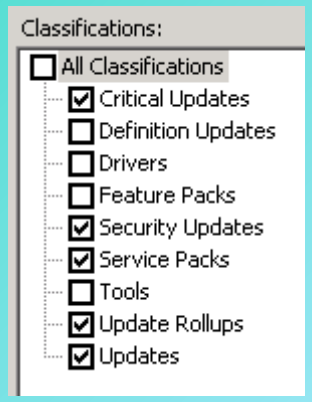
Spustí znovu průvodce nastavením

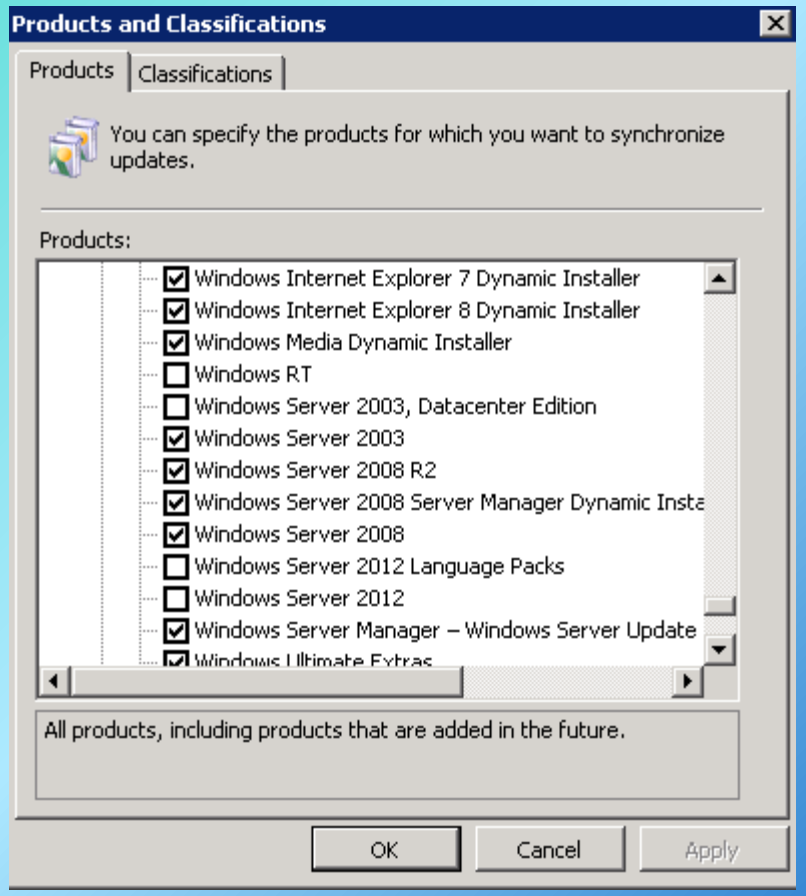
WSUS DC1 stahování a schvalování

WSUS downloaduje přes proxy:

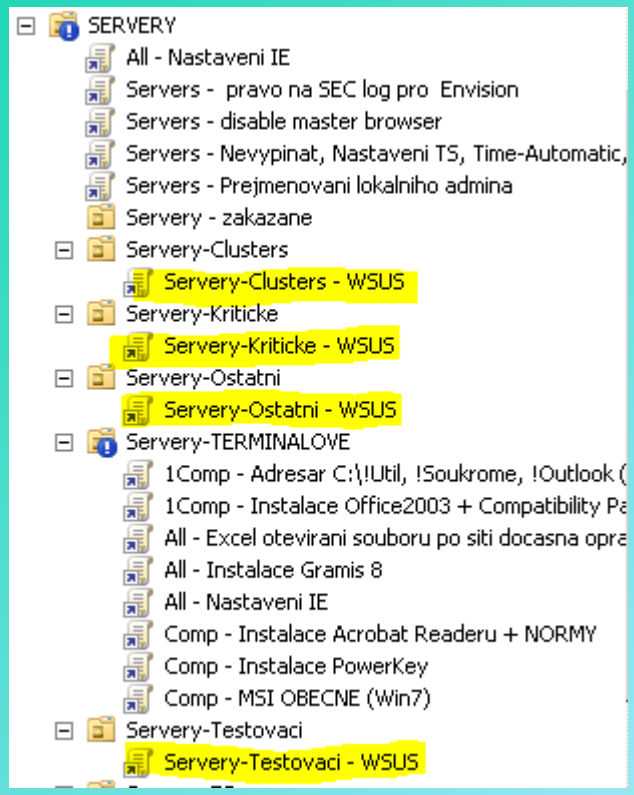


Produkty a klasifikace:
(options/product and classifications





WSUS nastavení přes GPO



WSUS je nastaven na řízení přes GPO. Nad kontejnery jsou Linkovány GPO objekty které řídí jednotlivá nastavení.

Povolením/zakázáním linku GPO řídíme aplikování patchů do prostředí pro jednotlivé kontejnery.

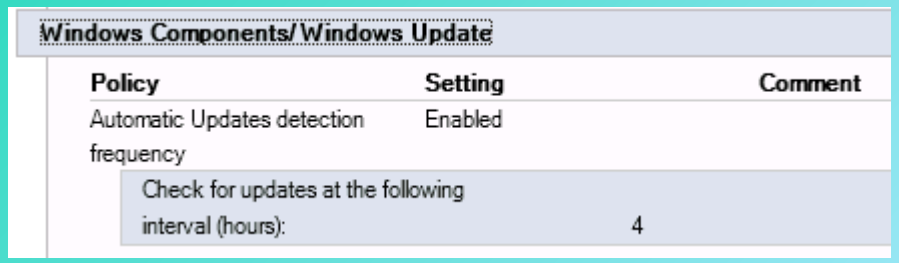
Server (ne DC) zařazený do OU aplikuje zásadu do 120 minut. Pro urychlení aplikování použijeme command:
gpudpate /force
Následně můžeme zkontrolovat zda je v registrech uložena Správná hodnota :

Name	Type	Data
(Default)	REG_SZ	(value not set)
TargetGroup	REG_SZ	Servery-Kriticke
TargetGroupEna...	REG_DWORD	0x00000001 (1)
WUServer	REG_SZ	http://dc1
WUStatusServer	REG_SZ	http://dc1

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate

WSUS klient

WSUS klient pravidelně nahlašuje svůj status WSUS serveru
WSUS klient pravidelně kontroluje schválené aktualizace



Windows Components/Windows Update		
Policy	**Setting**	**Comment**
Automatic Updates detection frequency	Enabled	
Check for updates at the following interval (hours):	4	

Pokud řadíme nového klienta, přesunujeme mezi OU, nebo řešíme problém, zavoláme commnad:
wuauclt /detectnow /reportnow

V konzoli pak vidíme čas kdy klient komunikoval z WSUS serverem:

Název	Adresa IP	Operační systém	Nainstalo...	Poslední hlášení o stavu
sysprep-pc	192.168.10.57	Windows 7 Professional	95%	27.1.2015 9:58

Zabezpečení WSUS

SSL – S MS se komunikuje přes SSL defaultně. U Downstream serveru lze zadat u adresy Upstream serveru

Oprávnění na filesystém (WSUS\WsusContent) - NT Authority\Network Service - Úplné řízení – provede instalace. Některé bezpečnostní programy to ale mohou vynulovat. Bez tohoto se nepodaří stáhnout službou BITS (Background Intelligent Transfer Service) data

V AD vytvořeny dvě skupiny
- *WSUS Administrators* – plná administrátorská oprávnění. Automaticky do nich patří Domain a Local Admins
- *WSUS Reporters* – Read only přístup (tj. i tvoření reportů)

Pokud je prostředí chráněno i zevnitř, je třeba povolit přístup na porty 80 a 443 na:

http://windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com
http://*.update.microsoft.com
http://*.windowsupdate.com
http://download.microsoft.com
http://wustat.windows.com
http://ntservicepack.microsoft.com
https://*.windowsupdate.microsoft.com
https://*.update.microsoft.com
http://download.windowsupdate.com
http://*.download.windowsupdate.com

WSUS 4.0 (Windows 2012) využívá už SHA256 hashes

WSUS základní činnosti

Definice updatů k stahování a distribuci
Schvalování automatické + manuální
Report stavu stanic/serverů
Čištění WSUS od nepotřebného smetí

→ WSUS OPTIONS

Cílení updatů
Úprava nastavení, chování, frekvence a času updatů
Krizové řízení (okamžité, co nejrychlejší atd.)

→ GPO/AD

Kontrola mimo reporty WSUS

→ MBSA

Features

Ruční import updatu
Pravé tl. na Updates
Import Updates
V katalogu Microsoft Update Catalog dát vyhledat
Zaškrtnout aktualizaci a kliknout na ADD
Vpravo nahoře do basketu a tam dát **Import directly into Windows Server Update Services** checkbox.

Odebrání aktualizace (Schválit – schváleno k odebrání)
Odebrány mohou být pouze aktualizace, které podporují odebrání. Před provedením tohoto kroku si prohlédněte informace v části **Lze odebrat** ve vlastnostech aktualizace (dole). Pokud jste zvolili k odebrání více než jednu aktualizaci a jedna nebo více aktualizací nepodporuje odebrání, bude akce odebrání použita pouze na aktualizace, které odebrání podporují. Lze kombinovat s termínem odebrání.

WSUS 4.0 – Podporuje SHA256 a kompletní ovládání přes PowerShell
https://docs.microsoft.com/en-us/powershell/module/wsus/?view=win10-ps

WSUS úskalí automatických aktualizací

- Vytvořit si testovací skupinu počítačů (odpovídajících vzorků).

- Produktů je tolik, že je nelze všechny v kombinaci testovat. Navíc úspory vedou k tomu, že se zákazníci stávají betatesteři.
- Výrobci HW (AMD, nVidia) již otevřeně kritizují Microsoft – nevídané
- Automatické schvalování nejsou již ve firmách doporučované. Dříve byl jeden až dva problémy za rok. Nyní jich je deset za posledních šest měsíců (KB2975331, 2975719, 2970228, 3002339, 2986475 …)

Problémy Microsoftu s aktualizacemi

AKTUALIZACE 2014	ČÍSLO	POZNÁMKA	PROBLÉM	OPRAVA	ŘEŠENÍ
SRPEN	KB 2975331	Hlavní aktualizace pro Windows 8 a RT	Chybová zpráva (0x50), modrá obrazovka, fonty se nezobrazují korektně.		Aktualizace opravena a znovu nabídnuta pod stejným číslem na konci srpna.
	KB 2975719	Hlavní systémová aktualizace pro Windows 8.1 a RT 8.1	Chybová zpráva (0x50), modrá obrazovka, fonty se nezobrazují korektně.		Aktualizace opravena a znovu nabídnuta pod stejným číslem na konci srpna.
	KB 2982791	Aktualizace pro Windows 7 a 8, opravující chybu při práci s fonty	Chybová zpráva (0x50), modrá obrazovka, fonty se nezobrazují korektně.		Nahrazena záplatou KB2993651, opravující všechny chyby, dostupnou na konci srpna.
	KB 2970228	Aktualizace pro Windows 7 a 8, umožňující zadání symbolu rublu pomocí klávesnice	Chybová zpráva (0x50), modrá obrazovka, fonty se nezobrazují korektně.		Chyba opravena záplatou KB2993651, poté znovu zveřejněna KB2970228.
ŘÍJEN	KB 2949927	Aktualizace pro Windows 7, doplňující podporu SHA-2	Jakmile je deaktivován Bitlocker, KB2949927 je automaticky odinstalována.		Doposud neexistuje žádné řešení.
	KB 3000061	Oprava pro ovladač na úrovni jádra ve Windows 7 a 8, uzavírající mezeru v souboru win32k.sys	Ovlivňuje Windows 8, když jsou instalovány jako aktualizace Windows 7; KB3000061 je automaticky po restartu odinstalována.		Uživatelé našli řešení: Instalace proběhne bez problémů, pokud smažete vybrané položky v registrech (viz následující strana).
	KB 3000869	Aktualizace pro Windows 7 a 8, uzavírající mezeru v rozhraní OLE (útok Sandworm)	Aktualizace neopravuje chybu.		Mezeru opravují KB3011443 a KB3010060. Po opravě je aktualizace znovu zveřejněna.
LIST.	KB 2992611	Aktualizace instalující nové šifrovací procedury pro Windows a Windows server	HTTPS spojení se servery využívajícími TLS 1.2 padá. Snížení výkonu u SQL serveru.		KB3018238 zveřejněná o týden později: Nové šifrovací metody jsou již aktivovány automaticky.
PROSINEC	KB 3004394	Oprava aktualizačního modulu kořenových certifikátů pro Windows 7 a 8	Systém se hroutí do modré obrazovky. Nelze instalovat ovladače. Nelze spouštět programy.		KB3024777 odinstaluje KB3004394. Doposud žádné jiné řešení.
	KB 3008923	Kumulativní bezpečnostní aktualizace pro Internet Explorer	IE9 padá. Dialogová pole se v Internet Exploreru 11 nezobrazují korektně.		KB3025390 odinstaluje KB3008923. Doposud žádné jiné řešení.
	KB 3011970	Aktualizace technologie Silverlight	Silverlight odmítá přehrávat DRM chráněný obsah.		Opraveno s novou verzí Silverlight. KB3011970 je znovu k dispozici.
	KB 2553154	Oprava chyb v programu Excel ve verzích 2007, 2010 a 2013	Aktualizace způsobuje problémy s makry, rozhraní ActiveX přestává fungovat.		Uživatelé našli řešení: odstranění souboru MSForms.exd.
	KB 2986475	Systémová aktualizace pro Exchange Server 2010 SP3	Outlook odmítá otevřít složku s odeslanou poštou a nelze ani odesílat nové zprávy.		Nouzové řešení: Přístup do Outlooku přes webové rozhraní.
	KB 3002339	Aktualizace pro Visual Studio 2012, opravující chyby v .NET	Aktualizace se opakuje v nekonečné smyčce.		Uživatelé našli řešení: manuální instalace záplaty.

Žádná Odstranění aktualizace

Řešení problémů

1) WSUS server

- C:\Program Files\Update Services\Tools\WsusUtil.exe

checkhealth

System Tools - Event Viewer - Custom Views - Server Roles – WSUS

healthmonitoring *ParametrName*

- C:\program files\update service\LogFiles (Logy WSUSu)

- C:\inetpub\logfiles

Řešení problémů

2) Klienti

- Urychlení napojení na WSUS (detekce WU a Report statusu)
wuauclt.exe / detectnow /reportnow

- Poradce při potížích se službou Windows Update
https://support.microsoft.com/cs-cz/help/4027322/windows-update-troubleshooter

- Log ve Windows 10 se už nevytváří v C:\Windows\WindowsUpdate.log
Nyní přes PowerShell - Get-WindowsUpdateLog

Další logy (přes eventvwr.exe):
C:\ProgramData\USOShared\Logs\UpdateSessionOrchestration.etl
C:\ProgramData\USOShared\Logs\NotificationUxBroker.etl
C:\Windows\Logs\WindowsUpdate*.etl TOTO BERE PowerShell - Get-WindowsUpdateLog

- Plus spousty dalších osvědčených postupů

WSUS informační zdroje a doporučení

- Nezapomenout pří instalaci nových produktů do domény upravit i WSUS.
- Používat jednotný DNS záznam pro možnost budoucího přemístění.
- S uvážením používat importování updatů.
- Pokročilejší WSUS - SCCM (přehlednější reporty, důvody chyb, opravy instalací …)

Step by step WSUS
http://technet.microsoft.com/en-us/library/dd939822(WS.10).aspx

How to check and change port
https://cloudmesh.wordpress.com/how-to-check-and-change-the-wsus-port/

WSUSUtil
https://docs.microsoft.com/de-de/security-updates/windowsupdateservices/18127651

Enable SSL
https://jackstromberg.com/2013/11/enabling-ssl-on-windows-server-update-services-wsus/

Change SQL database
https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/manage/wid-to-sql-migration

Windows 10 can’t update
https://www.alphr.com/microsoft/1001411/how-to-fix-windows-update-in-windows-10-if-it-becomes-stuck-1