

Desktop systémy Microsoft Windows

IW1/XMW1 2012/2013

Jan Fiedor

ifiedor@fit.vutbr.cz

Fakulta Informačních Technologií

Vysoké Učení Technické v Brně

Božetěchova 2, 612 66 Brno

Revize 2.10.2012

Správa bitových kopií systému

Offline servicing

- Modifikace obsahu bitové kopie bez nutnosti jejího nasazení a opětovného zachycení (uložení)
- Vyšší bezpečnost
 - Aplikace aktualizací před startem systému
- Není potřeba resetovat dobu aktivace Windows
- Možnost výměny souborů odpovědí
- Většina úprav prováděna nástrojem **DISM**

DISM

- Nástroj pro obsluhu WIM souborů a přípravu Windows PE bitových kopií
- Použití
 - Úprava Windows PE 3.0 / 4.0 bitových kopií
 - Povolení / zakázání funkcí systému Windows
 - Přidání / odebrání / vypsání balíků / ovladačů
 - Konfigurace oblastních a jazykových nastavení
 - Upgrade edice systému Windows
 - ...

Základní informace o bitových kopiích

- Informace o bitových kopiích ve WIM souboru
 - `dism /Get-WimInfo /WimFile:<cesta-k-wim> [/Index:<index> | /Name:<název>]` (WAIK)
 - `dism /Get-ImageInfo /ImageFile:<cesta-k-wim/vhd> [/Index:<index> | /Name:<název>]` (Windows ADK)
- Informace o všech připojených bitových kopiích
 - `dism /Get-MountedWimInfo` (WAIK)
 - `dism /Get-MountedImageInfo` (Windows ADK)

Připojení bitové kopie (WAIK)

- Připojení bitové kopie do zadaného adresáře
 - **dism /Mount-Wim /WimFile:<cesta-k-wim> {/Index:<index> | /Name:<název>} /MountDir:<adresář> [/ReadOnly] [/ScratchDir:<adresář>]**
 - Možnost definice adresáře pro uložení dočasných souborů (přepínač **/ScratchDir**)
 - Ve výchozím nastavení adresář **\<windows>\%Temp%**
 - Adresář musí být lokální
 - Obsah tohoto adresáře je vymazán po každé operaci

Připojení bitové kopie (Windows ADK)

- Připojení bitové kopie do zadaného adresáře
 - **dism /Mount-Image /ImageFile:<cesta-k-wim/vhd> {/Index:<index> | /Name:<název>} /MountDir:<adresář> [/ReadOnly] [/Optimize] [/CheckIntegrity] [/ScratchDir:<adresář>]**
 - Přepínač **/Optimize** urychlí připojení bitové kopie
 - Úkony prováděné při připojení budou provedeny při prvním přístupu k obsahu WIM resp. VHD souboru
 - Přepínač **/CheckIntegrity** ověří poškození (**pouze**) WIM souboru (**nelze** použít pro VHD soubory)
 - Pokud je poškozen, nebude bitová kopie připojena

Možnosti a omezení

- Bitové kopie ve WIM souborech nacházejících se na CD nebo DVD lze připojit pouze pro čtení
- Cílový adresář musí být prázdný
- Cílový adresář nesmí být symbolický odkaz
- Lze připojit maximálně 20 bitových kopií

Odpojení bitové kopie

- Odpojení bitové kopie ze zadaného adresáře
 - `dism /Unmount-Wim /MountDir:<adresář> {/Commit | /Discard} (WAIK)`
 - `dism /Unmount-Image /MountDir:<adresář> {/Commit | /Discard} [/CheckIntegrity] [/Append] (Windows ADK)`
- Přepínač **/Commit** vynutí uložení změn v bitové kopii před jejím odpojením (Přepínač **/Discard** je zahodí)
- Přepínač **/Append** uloží změny jako novou bitovou kopii ve WIM souboru (namísto přepsání původní)

Další možnosti obsluhy bitových kopií

- Uložení změn v bitové kopii do WIM souboru
 - **dism /Commit-Wim /MountDir:<adresář> (WAIK)**
 - **dism /Commit-Image /MountDir:<adresář> [/CheckIntegrity] [/Append] (Windows ADK)**
 - Časově náročná operace
- Obnova připojení bitové kopie v daném adresáři
 - **dism /Remount-Wim /MountDir:<adresář> (WAIK)**
 - **dism /Remount-Image /MountDir:<adresář> (Windows ADK)**

Údržba připojených bitových kopií

- Odstranění poškozených a nezapsaných souborů
 - **dism /Cleanup-Wim (WAIK)**
 - **dism /Cleanup-Mountpoints (Windows ADK)**
 - Provádí se u všech připojených bitových kopií
 - Neodpojí ani nesmaže připojené bitové kopie

Přepínače pro získávání informací

Přepínač	Popis
/Get-CurrentEdition	Zobrazí informace o edici systému Windows
/Get-StagedEditions	Zobrazí seznam edicí, jenž mohou být z bitové kopie odebrány
/Get-TargetEditions	Zobrazí seznam edicí, na které může být systém povýšen
/Get-Intl	Zobrazí nastavení oblasti a jazyka
/Get-Drivers	Zobrazí informace o všech <i>out-of-box</i> ovladačích
/Get-DriverInfo	Zobrazí informace o konkrétním ovladači
/Get-Packages	Zobrazí informace o všech balících
/Get-PackageInfo	Zobrazí informace o konkrétním balíku
/Get-Features	Zobrazí informace o všech funkcích (<i>features</i>)
/Get-FeatureInfo	Zobrazí informace o konkrétní funkci (<i>feature</i>)

Výše uvedené přepínače lze použít pro získávání informací o aktuálně běžícím systému (přepínač **/online**) i o systému uloženém v nějaké bitové kopii (přepínač **/image**)

Správa edicí operačního systému

- Změna edice systému Windows v bitové kopii
 - **dism /Image:<adresář> /Set-Edition:<id-edice>**
 - Bitová kopie musí obsahovat soubory dané edice
- Změna edice běžícího systému
 - **dism /Online /Set-Edition:<id-edice> /ProductKey:<licenční-klíč>**
 - Lze použít pouze u Windows Server
- Změna licenčního klíče v bitové kopii
 - **dism /Image:<adresář> /Set-ProductKey:<klíč>**

Správa jazyka operačního systému

Přepínač	Popis
/Set-UILang	Nastaví jazyk uživatelského rozhraní (jen pokud je nainstalován)
/Set-UILangFallback	Nastaví záložní (<i>fallback</i>) jazyk uživatelského rozhraní (potřeba jen pokud je hlavní jazyk tzv. částečně lokalizovaným jazykem)
/Set-SysLocale	Nastaví jazyk pro programy nepodporující sadu Unicode
/Set-UserLocale	Nastaví jazyk uživatelské lokalizace systému (formát měny, času)
/Set-InputLocale	Nastaví vstupní jazyk a rozložení klávesnice
/Set-LayeredDriver	Nastaví ovladač klávesnice (Korea, Japonsko mají jiné klávesnice)
/Set-TimeZone	Nastaví časovou zónu

Výše uvedené přepínače lze použít pouze pro systémy uložené v nějaké bitové kopii (přepínač **/image**)

Správa ovladačů

- Jsou podporovány jen ovladače ve formátu **.inf**
 - Nelze použít ovladače uložené v MSI balících nebo jiných instalačních balících (např. v EXE souborech)
- Spravovat lze pouze ovladače v offline bitových kopiích (připojených do nějakého adresáře)

Přidání ovladače do bitové kopie

- **dism /Add-Driver /Image:<adresář> /Driver:<adresář/cesta-k-inf> [/Recurse]**
- Pokud je zadán adresář s ovladači jsou přidány všechny ovladače v tomto adresáři
 - **/Recurse** pro zpracování i ovladačů v podadresářích
- Na 64-bitových verzích systému Windows musí být všechny ovladače digitálně podepsány
 - Instalaci nepodepsaných ovladačů je možné provést přidáním přepínače **/ForceUnsigned**

Odebrání ovladače z bitové kopie

- **dism /Remove-Driver /Image:<adresář> /Driver:<cesta-k-inf>**
- Nelze odebrat výchozí ovladače systému
- Soubory **.inf** přidaných ovladačů mají vždy název ve formátu **oem<číslo>.inf**
 - Pro vyhledání lze použít **dism /Get-Drivers**

Správa balíků operačního systému

- Jsou podporovány balíky ve formě **.cab** souborů a **.msu** (*Windows Update Stand-alone Installer*) souborů
- Balíky lze spravovat jak v offline bitové kopii, tak i v online (aktuálně běžícím) systému

Přidání balíku do bitové kopie

- **dism /Add-Package /Image:<adresář> /PackagePath:<cesta> [/IgnoreCheck]**
- Jako cestu lze zadat
 - Soubor **.msu** nebo **.cab**
 - Adresář s rozbaleným **.cab** archívem
 - Adresář obsahující jeden či více **.msu** a **.cab** souborů
- Balík musí být aplikovatelný na systém obsažený v cílové bitové kopii
 - Aplikaci balíku lze vynutit přepínačem **/IgnoreCheck**

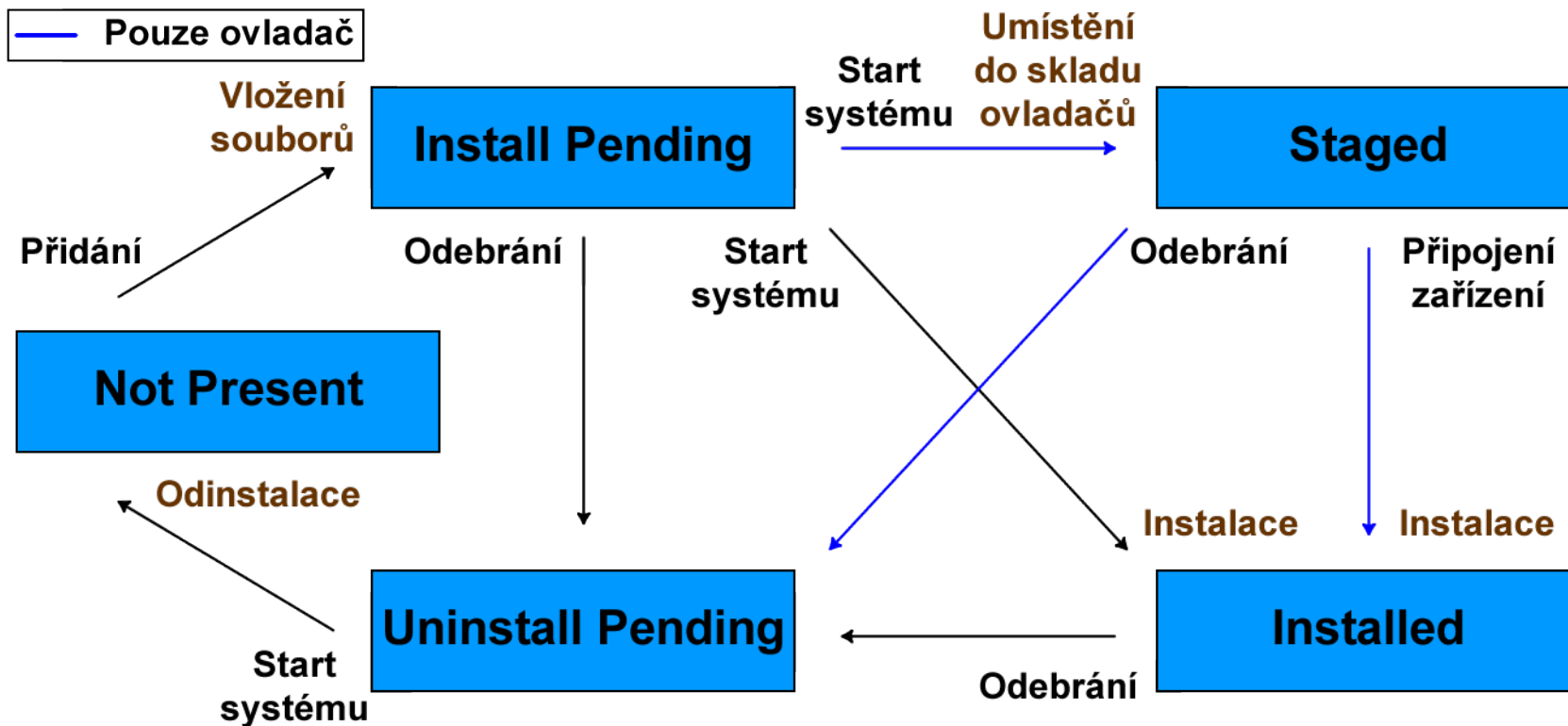
Průběh instalace balíků

- Přidané balíky jsou nainstalovány až při spuštění systému obsaženého v dané bitové kopii
- Pokud je instalace balíku závislá na přítomnosti jiných balíků, je lepší pro instalaci použít soubor odpovědí, kde lze definovat pořadí instalace
- Balíky jsou instalovány v pořadí v jakém jsou zadány na příkazové řádce

Odebrání balíku z bitové kopie

- **dism /Remove-Package /Image:<adresář> {/PackageName:<název> | /PackagePath:<cesta>}**
- Odebrat je možné jen balíky nainstalované z **.cab** souboru (balíky z **.msu** souboru nelze odebrat)
- Odebrané balíky jsou odinstalovány při spuštění dané bitové kopie

Stavy ovladačů a balíků



Správa funkcí operačního systému

- Povolení funkce (*feature*) operačního systému
 - **dism /Enable-Feature /FeatureName:<název>**
[/PackageName:<název>] [/PackagePath:<cesta>]
 - Přepínač **/PackagePath** lze použít pro instalaci balíku obsahujícího danou funkci
 - Nelze použít u **DISM** z **Windows ADK**
- Zakázání funkce (*feature*) operačního systému
 - **dism /Disable-Feature /FeatureName:<název>**
[/PackageName:<název>]

Správa aplikací

- Jsou podporovány pouze MSI aplikace (soubory **.msi**) a jejich záplaty (*patches*, soubory **.msp**)
 - Musí být nainstalované
- Identifikace pomocí GUID
- Nelze provádět instalace ani odinstalace
 - Jen získávání informací o aplikacích v offline bitových kopiích

Přepínače pro informace o aplikacích

Přepínač	Popis
/Get-Apps	Zobrazí základní informace o všech nainstalovaných MSI aplikacích
/Get-AppInfo	Zobrazí informace o konkrétní MSI aplikaci
/Get-AppPatches	Zobrazí základní informace o aplikovaných záplatách (<i>patches</i>) pro všechny nainstalované MSI aplikace
/Get-AppPatchInfo	Zobrazí informace o konkrétní záplatě (<i>patch</i>)
Výše uvedené přepínače lze použít pro získávání informací pouze o systému uloženém v nějaké bitové kopii (přepínač /image)	

Obsluha Windows PE bitových kopií

Přepínač	Popis
/Get-PESettings	Vypíše nastavení prostředí Windows PE
/Get-Profiling	Zjistí, zda je profilování zapnuto nebo vypnuto
/Enable-Profiling	Zapne profilování
/Disable-Profiling	Vypne profilování
/Apply-Profiles	Optimalizuje prostředí Windows PE
/Get-ScratchSpace	Zjistí velikost (v MB) RAM disku, jenž používá prostředí Windows PE
/Set-ScratchSpace	Nastaví velikost (v MB) RAM disku, jenž vytváří (a používá) prostředí Windows PE, lze nastavit jen velikosti 32, 64, 128, 256 nebo 512 MB
/Get-TargetPath	Zjistí kořenový adresář prostředí Windows PE
/Set-TargetPath	Nastaví kořenový adresář prostředí Windows PE, cesta k adresáři nesmí být delší než 32 znaků, musí být absolutní a bez mezer
Výše uvedené přepínače lze použít pouze pro prostředí Windows PE uložené v nějaké bitové kopii (přepínač /image)	

Aplikace souboru odpovědí

- **dism /Apply-Unattend:<*soubor-odpovědí*>**
- Spustí se **offlineServicing** konfigurační průchod
- Lze aplikovat na *online* i *offline* bitové kopie
 - Aktualizace ovladačů lze provádět pouze u *offline* bitových kopií
- Nekontroluje se aplikovatelnost balíčků

Nasazování bitových kopií systému

Tlustá bitová kopie (Thick Image)

- Kromě operačního systému obsahuje základní aplikace, jazykové balíky a další soubory
- Pro vytvoření lze použít MDT
- Jednoduché vytváření (minimum skriptování)
- Rychlé nasazení
- Pracná aktualizace
- Často se používá jako forma zálohy
 - Bootovatelné virtuální disky

Tenká bitová kopie (Thin Image)

- Obsahuje pouze operační systému (případně jen pár základních aplikací nebo jazykových balíčků)
- Složitější vytváření
 - Aplikace a jazykové balíky instalovány až dodatečně
 - Nutnost skriptování
 - Potřeba mít infrastrukturu pro distribuci aplikací
- Není nutné provádět aktualizace
- Nižší bezpečnost
 - Aktualizace aplikovány až po nasazení

Hybridní bitová kopie (Hybrid Image)

- Kombinace tlusté a tenké bitové kopie
 - Automatická instalace aplikací a jazykových balíčků při prvním startu systému (instalace ze síťového zdroje)
 - Výhody tenké bitové kopie, ale jednodušší vytváření
- Vyšší bezpečnost
 - Instalace před prvním přihlášením uživatele
- Není nutná infrastruktura pro distribuci aplikací
- Delší čas instalace
- Někdy jako tlustá bitová kopie rozšiřující tenkou

Light-Touch Instalace (LTI)

- Umožňuje výběr stupně automatizace
 - Může vyžadovat interakci s uživatelem
 - Riziko zavlečení chyb, nutnost mít oprávnění správce
- Minimální nároky na infrastrukturu
- Podpora nasazování ze sdíleného adresáře nebo odnímatelných úložišť (CD, DVD, UFD, ...)
- Nasazení může být zahájeno manuálně nebo automaticky pomocí WDS
- Rychlejší příprava procesu instalace

Zero-Touch Instalace (ZTI)

- Podporuje pouze plně automatizovaná nasazení
 - Žádná interakce s uživatelem
 - Nižší riziko zavlečení chyb
 - Oprávnění jsou uložena v konfiguračních souborech
- Vyžaduje System Center Configuration Manager
- Nasazování pouze z distribučních bodů SCCM
- Nasazení lze zahájit jen pomocí SCCM nebo WDS
- Složitější příprava procesu instalace
- Vyžaduje RPC pro komunikaci s klienty

User-Driven Instalace (UDI)

- Kombinace Zero-Touch a Light-Touch instalace
 - Prakticky „Zero-Touch s možností interakce uživatele“
- Vyžaduje System Center Configuration Manager
- Uživatel může zahájit i si přizpůsobit celý proces nasazování

Microsoft Deployment Toolkit (MDT)

- Sada nástrojů pro usnadnění nasazování systémů
 - Správa a distribuce bitových kopií (WIM souborů)
 - Správa ovladačů, aktualizací a aplikací
 - Řízení přístupu k distribučním sdílením
- Vyžaduje WAIK nebo Windows ADK
- Výše uvedené úkony realizují (resp. automatizují) tzv. sekvence úloh (*task sequences*)

MDT 2012 Update 1

- Podpora
 - Windows XP, Vista, 7 a 8
 - Windows Server 2003 (R2), 2008 (R2) a 2012
 - Windows PE 3.0 (WAIK) a 4.0 (Windows ADK)
- Podpora USMT 4.0 (WAIK) a 5.0 (Windows ADK)
 - Podpora hard-link migrace a stínových kopií
- Podpora instalace MS Office 2007, 2010 a 365
- Podpora Light-Touch instalace (LTI)
 - S SCCM i Zero-Touch (ZTI) a User-Driven (UDI)

Deployment Workbench

- MMC konzole pro práci s MDT
 - Vytváření a správa distribučních sdílení a bodů nasazení
 - Vytváření Windows PE bitových kopií pro Light-Touch instalaci
 - Definice sekvencí úloh (*task sequences*)
- Měla by běžet pouze jedna instance
 - Při běhu více instancí nepředvídatelné chování 😊

Distribuční sdílení (Distribution Share)

- Adresář obsahující soubory potřebné k instalaci a konfiguraci systému na cílovém počítači
 - Nastavení MDT
 - Bitové kopie (WIM soubory)
 - Zdrojové soubory sekvencí úloh, balíčků, aktualizací, jazykových balíčků, ovladačů a aplikací
 - Metadata operačních systémů a všech jejich balíčků, aplikací a ovladačů

Obsah distribučního sdílení

Adresář	Obsah
\$OEM\$	Potřeba pro zpětnou kompatibilitu s Windows XP a Server 2003
Applications	Instalační soubory aplikací
Backup	Záloha konfiguračních souborů MDT
Boot	Spouštěcí Windows PE bitové kopie (ve WIM a ISO formátech)
Captures	Zachycené (instalační) bitové kopie
Control	Konfigurační soubory MDT
Operating Systems	Bitové kopie
Out-of-Box Drivers	Ovladače
Packages	Balíky operačního systému a jazykové balíky
Scripts	Skripty využívané sekvencemi úloh (<i>task sequences</i>)
Tools	Nástroje pro vytváření, obsluhu a nasazování bitových kopií
USMT	Obsahuje User State Migration Tool

Body nasazení (Deployment Points)

- Zajišťují distribuci souborů z distribučního sdílení
- Každý bod nasazení umožňuje přístup k určité části souborů z distribučního sdílení
 - Pomocí tzv. výběrových profilů (*selection profiles*) lze definovat, které bitové kopie, ovladače, aktualizace, aplikace a sekvence úloh mají být k dispozici
- Klientské počítače se připojují k bodům nasazení a vybírají si sekvenci úloh, kterou chtějí spustit

Typy bodů nasazení

- Deployment Share (Single-Server, Lab)
 - Vytvoří bod nasazení z distribučního sdílení
- Linked Deployment Share (Separátní sdílení)
 - Vytvoří lokální nebo vzdálené sdílení obsahující část souborů z distribučního sdílení
 - Synchronizuje se s distribučním sdílením
- Media (Odnímatelné úložiště)
 - Vytvoří adresáře (nebo ISO) obsahující část souborů z distribučního úložiště

Sekvence úloh (Task Sequences)

- Sada úloh vykonávaných během nasazování
 - Řídí celý proces nasazování bitových kopií
 - Možnost slučování úloh do skupin
 - Úlohy lze vykonávat podmíněně
- Vytváří se z předdefinovaných šablon
- Vždy vázané na konkrétní bitovou kopii

Šablony sekvencí úloh (1)

Název	Popis
Sysprep and Capture	Zachycení zobecněného referenčního počítače
Standard Client Task Sequence	Výchozí sekvence úloh pro nasazování bitových kopií na klientské počítače / zachycení systému klientských počítačů do bitové kopie
Standard Client Replace Task Sequence	Zálohování systému a uživatelských dat a následné vymazání disku
Custom Task Sequence	Vlastní (uživatелеm definovaná) sekvence úloh, která neinstaluje žádný operační systém
Standard Server Task Sequence	Výchozí sekvence úloh pro nasazování bitových kopií na serverové počítače
Litetouch OEM Task Sequence	Nasazení bitových kopií na počítače v přípravném prostředí před jejich nasazením do produkčního prostředí (příprava <i>OEM images</i>)
Post OS Installation Task Sequence	Konfigurace systému po jeho nasazení (instalace aplikací, povolení technologie BitLocker, obnova uživatelských dat, ...)

Šablony sekvencí úloh (2)

Název	Popis
Deploy to VHD Client Task Sequence	Nasazení bitové kopie klientského systému na virtuální pevný disk (do VHD souboru) na cílovém počítači
Deploy to VHD Server Task Sequence	Nasazení bitové kopie serverového systému na virtuální pevný disk (do VHD souboru) na cílovém počítači

Základní úlohy

Úloha	Popis
Run Command Line	Vykoná zadaný příkaz
Run PowerShell Script	Spustí zadaný PowerShell skript
Set Task Sequence Variable	Nastaví proměnnou sekvence úloh, hodnoty proměnných ukládány v objektu Microsoft.SMS.TSEnvironment (přístupný ve skriptech)
Restart Computer	Restartuje počítač
Gather	Zpracuje nastavení obsažená v souboru ZTIGather.xml , případně v zadaném INI souboru (CustomSettings.ini , pokud není zadán)
Install Updates Offline	Nainstaluje vybrané balíky operačního systému a/nebo jazykové balíky, instalace v konfiguračním průchodu offlineServicing
Validate	Ověří, zda počítač splňuje podmínky pro nasazení systému
Install Application	Nainstaluje vybrané aplikace
Inject Drivers	Nainstaluje vybrané ovladače

Instalace aplikací

- Možnosti instalace aplikací
 - Instalace z distribučního sdílení
 - Instalace z externího zdroje
- Potřeba specifikovat příkaz pro instalaci aplikace
- Instalace více aplikací v jediném kroku
 - Vyžadované aplikace (nainstalovány automaticky)
 - Nastavení **MandatoryApplications** v **CustomSettings.ini**
 - Volitelné aplikace (uživatel určí, zda nainstalovat)
 - Nastavení **Applications** v **CustomSettings.ini**
 - Vložením informací do MDT databáze

System Center Configuration Manager

- Kompletní řešení pro správu systémů Windows
- Umožňuje
 - Nasazování operačních systémů, aplikací a aktualizací
 - Inventarizaci hardwaru a softwaru
 - Vzdálenou administraci systémů
 - Měření používání softwaru
 - ...
- Používá SQL Server pro uložení informací
 - Možnost využití informací MDT a jinými produkty

SCCM klienti

- Automatická detekce
 - Prohledávání sítě nebo databáze **Active Directory**
- Správa pomocí klientského softwaru
 - Nainstalován po detekci
- Rozdělení míst (*sites*)
 - Definice hranic pomocí IP nebo **Active Directory** míst
 - Sdílení konfigurace
 - Omezení komunikace na dané místo
 - Komunikace pomocí protokolů SMB, HTTP nebo HTTPS

Interoperabilita s MDT

- Sekvence úloh kompatibilní s MDT
 - Možnost exportu a importu
- Možnost Zero-Touch Instalace (ZTI)

Integrace SCCM a MDT

- 1) Nainstalovat MDT na každý počítač, na kterém běží **Configuration Manager Console**
- 2) Spustit **Configure ConfigMgr Integration Wizard**
 - Zaregistruje nové komponenty
 - Nainstaluje šablony sekvencí úloh pro ZTI
 - Přidá nové Windows Management Instrumentation (WMI) třídy
- 3) Spustit **Remove PXE Filter Wizard**
 - Odebere PXE filtry vytvořené staršími verzemi MDT