Univerzita Hradec Králové

Fakulta informatiky a managementu

Katedra informatiky a kvantitativních metod

IT management koncových stanic ZF Frýdlant

Diplomová práce

Autor: Luboš Hájek

Studijní obor: Aplikovaná informatika

Vedoucí práce: doc. RNDr. Petra Poulová, Ph.D.

Pracoviště: Katedra informatiky a kvantitativních metod

Hradec Králové Duben 2020

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 28. dubna 2020 ……..

Luboš Hájek

Poděkování

Chtěl bych poděkovat doc. RNDr. Petře Poulové, Ph.D. za vstřícnost a praktické rady, které mně pomohly při tvorbě této práce. Dále bych chtěl poděkovat všem členům IT a IS týmu v ZF Frýdlant, kteří mi tuto práci umožnili zpracovat a vytvořili příjemné pracovní prostředí.

Anotace

Luboš Hájek, IT management koncových stanic ZF Frýdlant, Diplomová práce, Fakulta Informatiky a managementu Univerzity Hradec Králové 2020.

Práce se zabývá představením a následnou implementací systému pro endpoint management ve firmě ZF Frýdlant. V práci je představena virtualizační platforma VMware ESXi a proces její implementace jako nástroje pro serverovou virtualizaci. Následuje instalace serverového operačního systému a aplikace nástroje pro endpoint management Symantec Altiris. V systému Altiris je prezentován proces vytvoření automatického nasazení operačního sytému Windows 10.

Klíčová slova: Endpoint management, VMware ESXi, Altiris, deployment.

Annotation

Luboš Hájek, IT endpoint management ZF Frýdlant Diploma Thesis, The Faculty of Informatics and management, The University of Hradec Kralove 2020.

The thesis deals about introduction and implementation of system for endpoint management in ZF Frýdlant company. In the thesis is introduced and implemented virtualization platform VMware ESXi. VMware is introduced like a tool for server virtualization. Installation of server operation system and deployment of Symantec Altiris system follow. In Altiris is presented process of creation automated package for Windows 10 deployment for endpoint devices.

Keywords: Endpoint management, VMware ESXi, Altiris, deployment.

Obsah

Cíle práce

Cílem této práce je představit řešení pro IT manažery a jejich podřízené v podobě systému pro endpoint management. V práci bude postupně přiblížen proces implementace a kroky s ní spojené i popis funkcionality daného systému. Práce si klade za cíl představení daného nástroje spolu s virtualizační platformou VMware ESXI ve společnosti ZF Frýdlant. Cíle práce zahrnují nasazení samotného virtualizačního nástroje VMware ESXi a veškeré s ním spojené úkony a technologie. Práce by dále měla představit nasazení nástroje Symantec Altiris pro endpoint management do dříve připraveného virtuálního prostředí VMware ESXi včetně technologií a nástrojů k tomu potřebných. Práce představí proces vytvoření softwarového balíku pro automatický deployment (nasazení) operačního systému Windows 10 pomocí implementovaného nástroje Altiris.

Struktura práce

Práce obsahuje klasickou strukturu, tedy úvod, hlavní část a závěr práce. Hlavní část práce je rozdělena na dvě základní části, a to teoretickou zvanou „Teorie", v jejímž rámci jsou popsány hlavní metody, technologie a nástroje použité v praktické části. Druhá část práce zobrazuje praktické nasazení a použití daných technologií a nástrojů v praxi. Tato část je nazvaná „Implementace".

Teoretická část práce se při popisu principů a technologií prolíná s praktickou, kde jsou tyto principy uplatněny. Jak v teoretické, tak i v implementační části práce se postupně prezentují dva hlavní nástroje, a to VMware ESXi pro serverovou virtualizaci a Symantec Altiris pro endpoint management.

1. Úvod

Velkými hráči dnešního světa jsou korporátní společnosti obrovských rozměrů. Tyto společnosti více či méně udávají směr, kterým se celá společnost v daném oboru ubírá. Vznik těchto gigantů by nebyl možný bez zařízení a technologií, jež jsou dnes obecně, ač v různé míře, dostupné. Jedná se o zařízení jako notebooky, telefony, tablety, stolní počítače, ale i pomyslná druhá strana, jako jsou servery, RAIDové pole, virtualizační nástroje, veškeré síťové prvky jako routery switche a tak dále. Vybavení korporace v tomto pohledu znamená pořízení stovek tisíc až milionů takovýchto zařízení za účelem sloužit zaměstnancům dané společnosti. Tato zařízení mají často své procesy či mechanismy na samosprávu, údržbu a aktualizace sebe samotných. Otázkou zůstává, pokud takovýto mechanismus existuje, do jaké míry je bezpečný a dostačující pro potřeby korporátu. A nabízejí se další otázky jako: Je tento mechanismus dostatečně flexibilní pro přizpůsobení danému uživateli? Lze tyto procesy alespoň u většiny těchto zařízení nějakým způsobem automatizovat? Je třeba jejich triviální správou zatěžovat uživatele nebo dokonce IT administrátory? Na většinu těchto otázek nelze jednoduše odpovědět, a tak vzniká potřeba vytvářet nástroje, které toto rozhodování dokáží ulehčit.

Dnešní zařízení, která jsou používána zaměstnanci korporátní společnosti, vykazují v určitých směrech vlastnosti odlišné od klasických domácích zařízení. Jeden z hlavních atributů, na který se většina korporátních společností zaměřuje a v čem se zpravidla liší korporátní zařízení od toho domácího, je bezpečnost. Bezpečnost firemních informací je klíčová pro udržení důležitého know-how firmy, přičemž každé zařízení s přístupem k těmto informacím v rukou uživatele představuje potenciální hrozbu pro únik informací.

Firmy často přicházejí s unikátními řešeními pro jednotnou správu všech těchto zařízení bez ohledu na typ, umístění, použití či další specifické atributy jednotlivých zařízení. Často marně hledají abstraktní vrstvu, jak co nejvíce zařízení spravovat jednotným řešením pro ušetření nákladů, času a energie na správu těchto zařízení. V mnoha případech vznikají upravená řešení pomocí skriptování a dalších nástrojů, které však nefungují konzistentně a vnáší pak do podnikové sítě bezpečnostní a další rizika.

Otázkou zůstává, zda vůbec existuje způsob, jak automaticky aktualizovat, spravovat a zabezpečovat takovou spoustu zařízení. Existuje-li nástroj, který by dokázal spravovat několik různých operačních systémů, od těch mobilních až po serverové. Odpověď je již známá a zní „ano“. Přesně pro tyto účely byly vyvinuty nástroje pro endpoint management, které slouží IT manažerům či IT administrátorům pro zefektivnění a automatizaci velkého počtu zařízení.

2. Teorie

V následující části práce jsou popsány nástroje, technologie, typy, metody, klady i omezení týkající se správy koncových zařízení. Navazující kapitola obsahuje jednak obecné pojednání o tom, proč je důležitá správa koncových zařízení, a také popis zúžené kategorie unifikované správy koncových zařízení. Následuje popis samotného nástroje Symantec Altiris jakožto nástroje pro správu koncových zařízení. Nakonec jsou zmíněny klíčové technologie pro pochopení funkce daného systému.

2.1. Obecná problematika správy koncových zařízení

Dnes již skoro bez výjimky práce v kanceláři, ať už je jakéhokoliv druhu, znamená práci s počítačem. Dnešní firmy, obzvláště ty působící v automotive průmyslu, dosahují v extrémních případech poměru jednoho koncového zařízení, například notebooku, desktopu či smart telefonu, na jednoho zaměstnance. Veškerá tato zařízení je třeba spravovat tak, aby jejich politika odpovídala nastaveným standardům dané společnosti. To nutí správce těchto zařízení k vytváření a následnému zefektivňování automatizovaných procesů k udržení stability, bezpečnosti a použitelnosti těchto koncových zařízení.

2.2. Proč endpoint management?

Stabilní, přesná a rychlá správa velké klientské infrastruktury není snadným úkolem. Po IT administrátorech se v každodenní praxi požaduje zavádění, přenos, instalace, opravy a následně aktualizování nových softwarů. Dalším z úkonů je řešení potíží v rámci podpory a provádění mnoha souvisejících činností. Tyto úkony se stávají ještě obtížnější v situacích, kdy se koncová zařízení nachází na odlehlých místech, s omezenými zdroji nebo s jakýmkoliv jiným přístupovým omezením. Náročnost těchto úkolů bez endpoint managementu (dále v práci také označování coby koncový či klientský management) úměrně roste s počtem koncových klientů. Již při malém počtu koncových zařízení se i obyčejná instalace nového softwaru stává nelehkým úkolem.

Efektivním způsobem, jak dosáhnout vysoké a udržitelné úrovně služeb a zabezpečení, je zajistit robustní infrastrukturu pro správu výše zmíněných operací, která by bez ohledu na umístění nebo vzájemnou vzdálenost mezi správcem

a koncovým zařízením umožnila provádět řadu úloh z jedné integrované konzole. Tato konzole by měla doménovým administrátorům umožnit efektivně kontrolovat velké množství koncových zařízení bez ohledu na jejich specifikace, jako jsou například poloha koncového zařízení, výpočetní výkon nebo dokonce operační systém koncového zařízení. [1]

Samozřejmě jsou zde i určitá omezení či požadavky, aby vůbec mohlo být dané zařízení spravováno samotným nástrojem. Za nejdůležitější lze považovat to, že musí být tomuto nástroji umožněn přístup do daného zařízení. V praxi to znamená, že dané zařízení nejlépe permanentně nebo minimálně jednou za stanovené období musí být připojeno do sítě tak, aby s daným zařízením mohl tento nástroj (zpravidla realizován určitým serverem) komunikovat. Samozřejmě daný nástroj musí mít administrátorský přístup k tomuto zařízení, bez čehož by nebylo možné na zařízení většinu potřebných úloh provádět. Z tohoto plynou i určitá bezpečnostní rizika.

2.3. Unified endpoint management (UEM)

Zde je vhodné začít definicí pro vytvoření alespoň částečné představy, co se za tímto názvem skrývá. Definici unified endpoint managementu (dále už jen UEM) dle článku Magic Quadrant for Unified Endpoint Management Tools [2] je možné chápat jako třídu softwarových nástrojů, která poskytuje integrované jednotné rozhraní pro správu firemních zařízení.

Nelze říci, zda je tato definice dost obsáhlá a komplexní, jelikož k UEM lze po krátkém hledání nalézt několik poměrně rozsáhlých definic, avšak všechny tyto definice se v podstatě shodují v tom, že UEM definuje většinu firemních zařízení jako „koncové body“. Správa těchto koncových bodů je centralizovaná a sjednocena jedinou aplikací. Tato aplikace poskytuje určitou konzoli, zpravidla prostřednictvím webového rozhraní, odkud je možné řídit veškeré procesy dané aplikace.

Pokud se podaří nástroj pro UEM úspěšně implementovat, poskytne nespočet výhod, a to zejména pro administrátory daných koncových zařízení. Základní výčet těch nejdůležitějších východ může vypadat následovně. [1], [3]

- UEM zajišťuje bezproblémový vzdálený přístup.
- Spravuje různá koncová zařízení s různým nastavením a operačními systémy.

- Centralizuje správu zařízení a zvyšuje produktivitu.
- Integruje bezpečnostní řešení a tak chrání IT infrastrukturu.
- Kontroluje hrozby způsobené malwarem nebo neautorizovaným přístupem.
- Spravuje veškeré aktualizace nasazených aplikací.
- Detekuje nově připojená zařízení do sítě.

Dále by bylo vhodné přesně definovat, co jsou to zmíněné koncové body neboli koncová zařízení. Daná zařízení jsou více či méně běžně používaná zařízení, jako například stolní počítače, notebooky, servery, tablety, chytré telefony, zařízení IoT (Internet of Things) nebo jakékoliv jiné zařízení používané zaměstnancem či hostem pro přístup do firemní sítě. [4] Coby koncové zařízení může být považován i například jakýkoliv stroj, který sbírá data o výsledcích výroby, testování nebo progresu výrobku, jako tomu je například ve společnosti ZF Frýdlant.

Každá skupina koncových zařízení má své specifické charakteristiky. Z toho důvodu je nutné ke každé jednotlivé skupině přistupovat specificky. Jako hlavní charakteristiku koncového zařízení lze označit jeho operační systém. Operačních systémů je celá řada, od těch jednodušších pro malé IoT zařízení, jako je například Raspbian, až po komplexní, kupříkladu macOS či hojně používaný Windows 10. Vždy před výběrem UEM nástroje je vhodné analyzovat portfolio operačních systémů, které je třeba spravovat, a tento fakt reflektovat ve výběru daného nástroje, tak aby daný nástroj přistupoval ke všem spravovaným operačním systémům, jak je žádoucí.

Od daného operačního systému se odvíjí i sada funkcí, které poskytují nástroje pro UEM (Jiné možnosti správy mají Raspbian, Android nebo například Windows 10). V poslední době se výrobci UEM řešení orientují převážně na mobilní zařízení, která jsou třeba spravovat důkladněji než ta, která neopustí prostory pracoviště či kanceláře. Jelikož jsou na správu mobilního zařízení kladeny výrazně vyšší nároky, jsou jednotlivé služby, které poskytují nástroje UEM, velice kritické z hlediska udržitelnosti daného zařízení. Jednotlivé služby, které je třeba zajistit při správě mobilního zařízení, lze kategorizovat. Ačkoliv se jednotlivé názvy kategorií můžou od různých poskytovatelů řešení UEM lišit, v podstatě se jedná o následujících pět funkcí v různých variantách. Tyto varianty nejlépe shrnuje kniha K. Hesse. [1], [5], [6]

2.3.1.1. Mobile device management (MDM)

Mobile device management zahrnuje životní cyklus mobilního koncového zařízení, a to nasazení, správu, vzdálený přístup, vyřazení z provozu, vzdálené vymazání a evidenci. Příkladem takového zařízení může být mobilní telefon, tablet, případně notebook, který zaměstnanec dostane i k osobnímu použití. Při přidělení zařízení se do telefonu či notebooku zavede aplikace spravující dané zařízení, která zpravidla dovolí uživateli jen ty operace, které jsou povoleny firemní politikou. Následně je zařízení s tímto aktivním softwarem používáno, aktualizováno a spravováno daným administrátorem. Ve chvíli, kdy se zařízení dostane do konce své životnosti (ať už z jakéhokoliv důvodu, například zastarání nebo i krádež), jsou správcem vzdáleně smazána veškerá firemní data a zařízení je vyřazeno.

2.3.1.2. Mobile application management (MAM)

Mobile application management spravuje veškeré aplikace v zařízení. Aplikuje nastavenou firemní politiku v daném zařízení. Poskytuje možnosti jako například takzvaný „whitelist“ či „blacklist“ [7], který si lze představit jako zakázání určitých aplikací na černé listině, nebo v opačném případě zakázání všech a povolení pouze vybraných aplikací na bílé listině. Jak již to u UEM bývá zvykem, podporuje hromadnou distribuci, a to jak nastavených pravidel, tak jednotlivého softwaru a aplikací. Velkou silou MAM je fakt, že zpravidla umožňuje izolovat určité aplikace od ostatních. A to tak, aby do daných aplikací neměly ostatní aplikace či jiný software jakýkoliv přístup. Toto se velmi hodí například při interně vyvinutých aplikacích, které zpravidla operují s velmi citlivými daty. Tyto aplikace včetně jejich dat lze pomocí MAM spravovat zcela izolovaně.

2.3.1.3. Mobile content management (MCM)

Mobile content management spravuje pravidla a zásady společnosti pro přístup k datům dané společnosti skrze mobilní zařízení. Jedná se o přístup k datům společnosti, která jsou reprezentována převážně soubory, či přístup do aplikací s daty dané společnosti. Jedná se převážně o velmi citlivá data s nutnou extrémní úrovní zabezpečení, ke kterým může mít mobilní přístup pouze omezená skupina lidí či dokonce nikdo. MCM zajišťuje řízení těchto přístupů.

2.3.1.4. Identity and access management

Identity and access management zajišťuje to, že pouze důvěryhodné a vhodně zabezpečené subjekty mohou získat přístup k firemním datům. Pod touto správou si lze představit technologie jako například single sign-on (SSO), které výrazně ulehčují autentifikaci uživatele ve firemním prostředí. Dále identity and access management zajišťuje správu a ověření certifikátů či takzvaný context-based access čili přístup založený na kontextu. Více o context-based řízení přístupu se lze dozvědět například z odborného článku Context-based Access Control Systems for Mobile Devices. [8] Context-based access pomáhá zlepšovat zabezpečení během autorizace a autentifikace pomocí registrace určitého zařízení s konkrétním uživatelem. Následně pomocí určitých vzorů chování uživatele vypočítává riziko, na základě kterého následně rozhodne, zda povolí či zamítne přístup k určitému zdroji.

2.3.1.5. Containment

V každém zařízení více či méně dochází k prolnutí osobního a firemního použití. Toto může mít za následek mísení a následný únik firemních dat. Nástroje UEM dovolují administrátorům efektivně oddělit aplikace, včetně dat na firemní a osobní, tak aby se co nejvíce zajistila jejich separace. Containment se týká zejména multimediálního obsahu, který taktéž může obsahovat citlivá data a je ho potřeba určitým způsobem chránit. Containment zajišťuje právě tuto ochranu.

Závěr UEM by mohl znít následovně. Použitím UEM se IT infrastruktura v dané společnosti transformuje z nepřehledného chaosu na konzistentní, přehlednou, bezpečnou a přitom stále flexibilní síť, která napomáhá ke zvýšení produktivity všech uživatelů v dané síti.

Určitá část endpoint managementu zde doposud nebyla zmíněna, avšak její zařazení je nanejvýš vhodné. Tato část se týká specifického okruhu zařízení, která se mohou nacházet v podnikové síti, avšak daný podnik je nemusí vlastnit ani mít pod svojí plnou správou. Otázkou je, proč by takové zařízení mělo v síti existovat. V dnešní době je běžné přinést si vlastní zařízení jako například chytrý telefon či méně často notebook do zaměstnání. Na daném pracovišti či v dané kanceláři se samozřejmě připojit ideálně na bezdrátovou firemní síť. Když už je zařízení připojeno do firemní

sítě, vyvstává nápad, proč si vlastně nepřidat do zařízení i například emailového klienta nebo pár firemních souborů pro přístup z domova. Laická úvaha je jasná. Je to přeci jednoduché, rychlé a bez problému. Avšak otázkou zůstává, zda takováto firemní data jsou zcela v bezpečí. Je tedy konkrétní zařízení zcela bezpečné? Je jeho software aktuální? Jsou instalovány pouze ověřené aplikace? Nebude s daty nijak jinak manipulováno?

Na tyto otázky správce firemní sítě nedokáže odpovědět. Jednoduše proto, že dané zařízení není pod jeho správou, ale pod správou majitele tohoto zařízení. Řešení vzniklého problému se pak částečně skrývá pod slovem BYOD.

2.3.2. BYOD

Předtím než bude vysvětlen pojem BYOD, je důležité objasnit kontext daných zařízení, která toto slovo zahrnuje. Ve vysvětlení se může zdát, že se určité časti či definice kryjí s již zmíněnými částmi UEM, například MDM aj. Avšak je třeba si uvědomit, že BYOD se týká soukromých zařízení, která jsou přinesena do firemního prostředí oproti již zmíněným metodám, které se týkají zejména zařízení, která jsou vlastněna a plně spravována danou společností.

Samotný BYOD je akronymem pro „bring your own device", přičemž počeštěný název je uváděn jako „přines si vlastní zařízení". Konkrétní definice by mohla znít následovně. BYOD je koncept, který zaměstnancům umožnuje využívat jejich osobní (vlastněná) zařízení pro připojení se k síti společnosti, pro přístup k datům společnosti a provádět úkony s tím spojené. [9] Tento fenomén se u nás začal rozvíjet po roce 2010, přičemž dnes již tento standard přijala většina větších společností za svůj.

Je však třeba pamatovat na to, že jako obecně všechno, i BYOD má dvě strany mince. Na jednu stranu je zde nepřeberné množství výhod, které přináší, jako například rapidní snížení nákladů na správu a pořízení daného hardwaru. Také zkracuje nutnou dobu zaškolení zaměstnanců pro dané zařízení téměř na nulu nebo například dává každému zaměstnanci možnost pracovat s poslední nejaktuálnější verzí softwaru v době, kdy celá organizace může ještě z nějakého důvod fungovat na starší verzi. [9], [10] Byť se tomu zpravidla konfigurace celé sítě BYOD snaží zabránit. Pomyslnou druhou stranu mince tvoří souhrnně řečeno oblast security a privacy. Jsou-li totiž

do zařízení stahována, či skrze zařízení je přistupováno k firemním datům, vždy existuje určité riziko ztráty nebo odcizení dat. Obzvláště pokud firemní data opouštějí dennodenně prostory společnosti v desítkách, někdy až stovkách nehomogenních soukromých zařízení. Nejedná se pouze o firemní data, ale i o situace, kdy zařízení vlastněné zaměstnancem může fungovat jako brána do firemní sítě. V případě, že dané zařízení bude nakaženo určitým typem malwaru, může to ve firemní síti způsobit jeho rozšíření na další přítomná zařízení. Tímto vzniká velké ohrožení, které může vést až k rozsáhlým škodám v celé firemní síti. Napadení, ochromení či odcizení dat z firemní sítě je nepřípustné a může eskalovat až do destrukce celé společnosti.

Tomuto se BYOD snaží zabránit hned několika způsoby. Jednak vynucováním bezpečnostních zásad na připojených zařízeních, jako jsou hesla pro odemčení, šifrování firemních dat a omezování přístupů. Na BYOD zařízení jsou zpravidla aplikovány větší nároky na ověření při přístupu k citlivým datům.

Dále pak nuceným instalováním antiviru, podpůrných softwarů pro detekci malwaru a klienta pro správu daného zařízení. K tomuto můžou částečně sloužit i nástroje pro již zmíněný koncový management, avšak zde správu těchto zařízení z velké části komplikuje heterogenita daných zařízení, která se zde vyskytuje. [11]

Na závěr řešení této problematiky lze říci, že BYOD přináší nesporné výhody pro společnost, která tento koncept implementuje. Avšak je třeba uvědomovat si veškerá rizika a pokusit se je minimalizovat již známými nástroji. Z hlediska bezpečnosti je vždy třeba zvážit přínos bezpečnosti oproti použitelnosti zařízení. Jelikož plně zabezpečené zařízení, zamknuté v trezoru a odpojené od sítě je sice bezpečné, ale zároveň nepoužitelné. Proto je vždy třeba hledat kompromis mezi bezpečností a použitelností.

Jak již bylo řečeno, celkovou správu koncových zařízení pomáhá administrátorům výrazně ulehčit několik speciálních nástrojů přímo pro to určených. Někteří výrobci softwaru poskytující ucelené balíky pro IT management, které zahrnují kromě jiného i nástroje pro správu koncových zařízení. Jedním z těchto poskytovatelů softwaru je Symantec se svým IT management suite.

2.4. Symantec IT management suite

Symantec IT management suite (ITMS) [12] je soubor nástrojů od firmy Symantec poskytovaný IT správcům pro IT management. ITMS kombinuje najednou několik nástrojů pro správu klientů, serverů, OS deploymentu a automatickou instalaci softwaru zároveň. Tyto nástroje slouží zejména pro zařízení, jako jsou stolní počítače, notebooky, tenké klienty, zobrazovače a servery. Většinu poskytovaných funkcí ITMS lze spravovat prostřednictvím jedné integrované, centrální konzole. Takováto platforma výrazně zjednodušuje, automatizuje, zefektivňuje správu a chod IT. Důležité je zmínit, že ITMS pracuje převážně v heterogenním prostředí vztaženém na typ zařízení. Kdy většina spravovaných zařízení je definována v určitém firemním standardu, kde jsou výčtem řečeny všechny modely a konkrétní typy povolených zařízení. [13]

Praxe ukazuje, že s neustále narůstajícím počtem koncových zařízení je třeba většinu operací, které jsou prováděny pravidelně na každém zařízení, centralizovat a následně automatizovat. Pokud by tyto operace nebyly automatizovány, chod IT by se postupně stával neudržitelným. Za pomyslnou alfu a omegu automatizace, bez níž by si dnes již mnoho IT správců nedovedlo představit svou náplň práce, lze označit auto deployment operačního systému, s následnou automatickou instalací potřebných softwarových balíčků. Pro tyto nejednoduché operace má Symantec ITMS nástroj zvaný Altiris.

2.4.1. Altiris

Altiris je integrovaný, standardizovaný nástroj patřící do skupiny nástrojů pro endpoint management, zároveň zastává funkci OS deploymentu a následné automatické instalace softwaru. Altiris umožňuje vytvářet a následně nasadit obrazy disků, migrovat data, konfigurace a cele systémy založené na operačních systémech Windows, MacOS či Linux. Altiris umožňuje takzvaný Ghost systém čili kdykoliv je vytvořený standardní referenční systém, lze ho jednoduše hromadně distribuovat na všechna ostatní zařízení v síti, a to nezávisle na hardwaru, na nějž má být nasazen.

Avšak je třeba pamatovat na to, že každý operační systém je z určitého pohledu jedinečný, proto lze individuálně konfigurovat jména zařízení, SID, IP adresy a další

nastavení. Samotná kategorie individualizace je licencování, a to jak operačního systému, tak instalovaných softwarových balíčku. Toto licencování je Altirisem taktéž podporováno, nicméně vyžaduje hlubší znalost licencovaného softwaru a jeho nastavení. Čerpáno z brožury Symantec data sheet [14], vybrané klíčové vlastnosti systému Altiris ze stejnojmenné brožury mohou vypadat následovně.

- Jednotné řešení pro stolní počítače, servery i notebooky.
- Podpora technologií jako PXE nebo Wake on LAN.
- Podpora pre-boot prostředí jako například Windows PE.
- Podpora hardwarově nezávislého deploymentu.
- Možnost konfigurace počítače pomocí image nebo skriptování.
- Integrace s ostatními nástroji Symantec.
- Podpora správy virtuálních strojů.

Zde je třeba zmínit, že výše uvedený Wake on LAN je velice užitečný, v praxi používaný síťový standard, který umožňuje správcům sítě zapnout koncová zařízení (zde myšleno zejména stolní počítače a notebooky) vzdáleně skrze určité rozhraní. Toto je hojně používáno správci například při instalaci nového softwarového balíčku pro všechny počítače v síti, přičemž je potřeba, aby nejlépe všechny počítače byly v daný čas zapnuté. Tyto procesy se zpravidla automatizují. To v praxi funguje tak, že správce před odchodem domů nastaví na určitý čas (ideálně čas, kdy nejsou daná zařízení používána) zapnutí všech koncových zařízení, následnou instalaci softwarového balíčku a vypnutí koncových zařízení. Příští den si nechá zobrazit report, na kterých zařízeních nemohl být software z nějakého důvodu nainstalován (zpravidla se vždy alespoň jedno zařízení najde), a takováto zařízení jsou pak řešena individuálně, například pomocí ruční instalace.

Zápor nejen Altirisu, ale i dalších nástrojů implementujících standard Wake on Lan lze velice abstraktně vyjádřit tak, že je třeba, aby tuto podporu, tedy Wake on Lan, měla hardwarově implementovanou síťová karta i základní deska koncového počítače, na které je zpravidla daná síťová karta integrovaná. [15] Což v případě novějších počítačů není až tak neobvyklé, ale ne samozřejmé. Ve chvíli, kdy koncový počítač daný standard podporuje, je zde druhé, sice banální, ale velice frustrující úskalí, které čeká na IT správce. Je třeba, aby tato možnost (probuzení pomocí síťové

karty) byla povolena v BIOSu (basic input/output systém). Což nevypadá na zásadní problém, avšak při nekonzistenci nastavení BIOSu dodávaného od výrobce, nebo například velké heterogenitě zařízení může docházet k problémům vypnutého Wake on LAN u celé řady koncových zařízení. V neposlední řadě je důležité, aby tento standard podporovaly i veškeré routery a další zařízení v síti. Což u routerů v domácím prostředí může být problém, avšak většina profesionálních řad tento standard již delší dobu bez problému implementuje.

Jako pokračování záporů Altirisu – jedna z mála, i když nelze říci striktně záporů, spíše pro někoho důvodu k zaražení je fakt, že Altiris je starší nástroj, než by se dalo čekat. Stejnojmenná společnost Altiris byla dvěma zakladateli založena v roce 1998, [16] následně 6. dubna v roce 2007 [17] byla odkoupena společností Symantec a do dnešní doby se název Altiris dochoval spíše jako pojmenování nástroje pro endpoint management než jako název dané společnosti.

Jak již bylo řečeno, je možné si všimnout, že v této práci popisovaný Altiris je tedy o něco starší než dnes běžně dostupné nástroje pro endpoint management. Avšak k nasazení tohoto nástroje bylo hned několik důvodů. Prvním a zároveň jedním z nejdůležitějších faktů pro nasazení Altirisu je předpis korporátní směrnice, kdy řešení pomocí nástrojů od firmy Symantec bylo předepsáno zde platným předpisem. V IT korporátním světě se jednoduše ne vždy implementují úplné novinky. Častokrát se nechává prostor již zaběhnutým, praxí prověřeným softwarům, které zaručují spolehlivost a bezproblémový provoz. Což byl druhý důvod pro implementaci Altirisu. Je sice starší, avšak o to více prověřený software pro již zmíněné úlohy, což poskytovalo nemalou výhodu ve stabilitě systému a velikosti komunity pro případné řešení překážek.

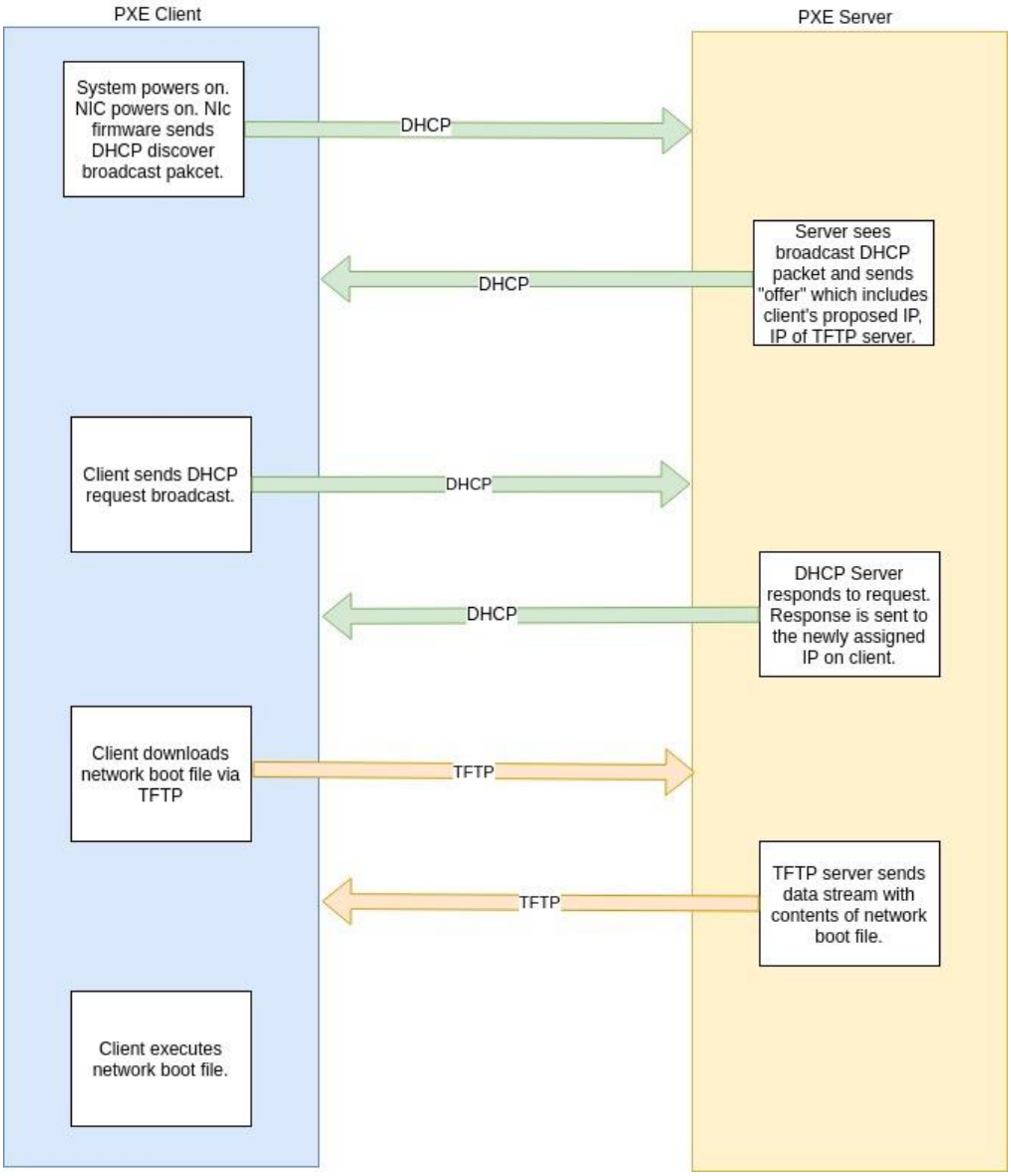
Jako další zmíněná technologie, kterou podporuje Symantec Altiris, je PXE. Jelikož PXE a další technologie jako UEFI a tak dále hrají významnou roli v automatickém deploymentu operačního systému, je vhodné je zde alespoň stručně zmínit.

2.5. Preboot Execution Environment (PXE)

Preboot execution environment (dále jen PXE) je prostření nebo je možné říci specifikace od společnosti Intel Corporation, která popisuje standardizované

prostředí klient – server. Toto prostředí umožňuje bootování (start operačního systému, zpravidla míněno zavádění jádra operačního systému) z počítačové sítě. Tato technologie je využívána různými softwary pro centrální IT management, zejména pro automatickou instalaci operačního systému případně pro tenké klienty. Přesný popis technologie lze najít ve specifikaci PXE. [18]

Zmíněný přesný popis funkce PXE je velice komplexní, vysvětlovat kompletní funkcionalitu by mohlo být redundantní. Avšak bude zde naznačen jednoduchý princip funkcionality pro představu procesu startu operačního systému ze síťového prostředí. Celý proces nejlépe vystihuje následující flow diagram z webové stránky linuxhit.com [19]



Obrázek 1 - Princip PXE zdroj: linuxhit.com [19]

Na obrázku lze vidět zjednodušené kroky celého procesu startu z PXE. [19] Začátek je dle specifikace DHCP protokolu klasické získání síťové konfigurace z DHCP serveru. Po kterém následuje stažení a spuštění daného souboru pro zavedení operačního systému z TFTP serveru. Jednotlivé kroky vypadají následovně.

- Zapnutí klienta a kompatibilního NIC (network interface controller).
- Klient vyšle „DHCP discover broadcast paket“, což indikuje potřebu získání síťové konfigurace.
- DHCP server broadcastem pošle odpověď, jíž se říká „offer“ neboli nabídka síťové konfigurace zahrnující i informace o TFTP serveru.
- Klient v této situaci nabídku zpravidla přijme a znovu broadcastem odešle potvrzení.
- DHCP server odesílá přiřazenou IP adresu a další nastavení.
- Klient dle získané konfigurace z DHCP žádá TFTP server o soubor pro start daného systému.
- TFTP server odesílá soubor.
- Klient daný soubor přijímá, ukládá a spouští.

Je vhodné si všimnout, že je využíván TFTP (trivial file transfer protocol) oproti klasickému FTP (file transfer protocol), které je sofistikovanější, ale zpravidla vyžaduje ověření a další záležitosti, které by daný proces komplikovaly.

Jako nevýhodu PXE oproti klasickému zavedení systému například z USB zařízení lze označit právě to, že PXE vyžaduje kompatibilní network interface controller (NIC) a sadu standardních síťových protokolů/serverů jako DHCP a TFTP. A proto je PXE rozšířeno převážně v IT a jiných centrech. Jak říká Kniha The Policy Driven Data Center with ACI. [20] V moderních datových centrech je PXE nejčastější a dalo by se říci, že i prozatím nejefektivnější volbou pro spouštění, instalaci a nasazení operačního systému.

2.6. Unified extensible firmware interface (UEFI)

Článek MS denied secure boot will exclude Linux od Johna Leydena [21] ve zkratce říká, že UEFI je specifikace, která definuje softwarové rozhraní mezi operačním systémem a firmware daného hardwaru. UEFI nahrazuje původní rozhraní zvané jako Basic Input – Output System (BIOS). Toto původní rozhraní bylo v různých verzích přítomné ve většině osobních počítačů od svého představení v roce 1975 až po současnost.

UEFI je stejně jako BIOS nainstalováno výrobcem základní desky a je prvním programem, který se spustí po zapnutí počítače. Z důvodu, že UEFI je programovatelné, umožňuje výrobcům jednotlivých počítačových komponent přidávat svoje ovladače přímo do rozhraní UEFI a následně je předat danému operačnímu systému, což UEFI posouvá z pozice obyčejného zavaděče do pozice, dalo by se říci lehkého operačního systému.

Jak je možné dočíst se v knize Beyond BIOS, [22] nejenže UEFI stále poskytuje podporu pro starší implementaci BIOS, ale také může podporovat vzdálenou diagnostiku a opravy počítačů. A to i bez nutnosti nainstalovaného operačního systému, což původní systém BIOS neumožňoval.

Coby jeden z největších přínosů a hlavních důvodů přechodu na UEFI se dá označit podpora GPT standardu pro členění disku. GTP (GUID Partition Table) standard přináší možnost zavedení operačního systému z větších disků než jsou 2TB oproti staršímu členění MBR (Master boot record), který toto zkrátka neumožňoval. [23]

Další část práce bude věnována podrobnějšímu popisu protokolu HTTP, a zejména jeho bezpečnější variantě HTTPS, a to hned z několika důvodů. Prvním důvodem ke zmínění těchto protokolů je obecná všudypřítomnost těchto protokolů. Dále v práci budou prezentovány VMware ESXI jako virtualizační nástroj spolu s konzolí pro enpoint managemet. Tyto dva nástroje jsou spravovány převážně skrze webové rozhraní. Právě tato webová rozhraní využívají zmíněné HTTP a HTTPS protokoly. Proto je dobré mít povědomost o těchto protokolech a jejich bezpečnosti. Neméně podstatným důvodem pro představení těchto protokolů je pak obecný fakt, že nejen

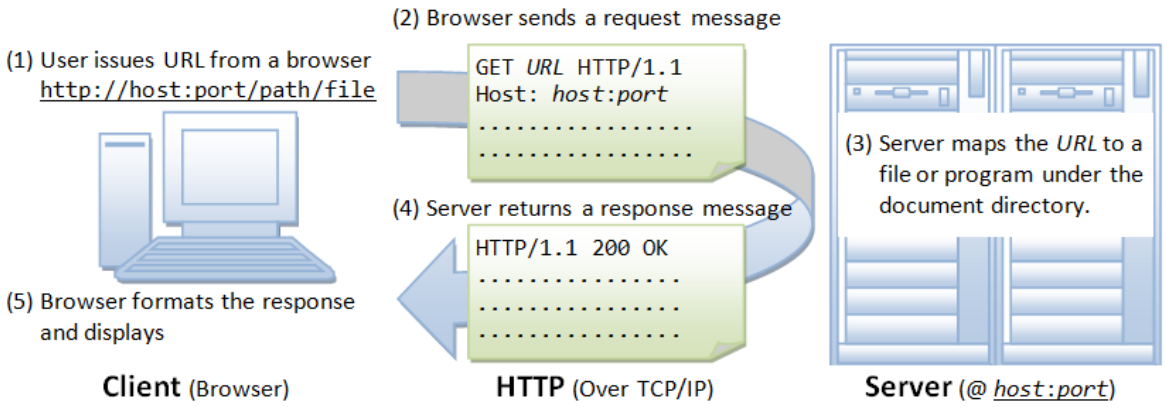
v ZF Frýdlant, ale i v ostatních společnostech se klade čím dál větší důraz na zabezpečení počítačových sítí. K tomuto zabezpečení výrazně přispívá právě protokol HTTPS, který je klíčovou součástí každé dobře zabezpečené webové aplikace.

2.7. HTTP a HTTPS protokoly

HTTP a HTTPS jsou internetové protokoly. Pro objasnění těchto protokolů je nejprve potřeba definovat pojem protokol jako takový. Protokol je soubor pravidel nebo také domluv, podle kterých probíhá komunikace mezi dvěma či více účastníky dané komunikace. Jak uvádí server techterms.com, protokol je soubor zavedených pravidel, která určují formát přenášených dat tak, aby oba účastníci (zpravidla klient a server) komunikaci rozuměli. [24] Jelikož se pomocí protokolu přenáší převážně data mezi klientem a serverem, hraje použitý protokol významnou roli v zabezpečení webových konzolí a aplikací. Tento fakt umocňuje to, že http a https ještě společně s SMTP protokolem (elektronická pošta) jsou nejrozšířenějšími internetovými protokoly, které slouží pro komunikaci na WWW (World Wide Web). Jeden z nejbezpečnějších z těchto protokolů je protokol HTTPS. Jedná se v podstatě o protokol http zabezpečený pomocí TLS protokolu (u starších verzí SSL protokolu), proto bude nejprve popsána funkce protokolu http a následně jeho modifikace https pomocí TLS.

2.8. Popis protokolů

HTTP je bezstavový protokol používající zpravidla TCP port 80. Kompletní definici všech internetových protokolů včetně http i https lze najít v oficiálních RFC (Request For Comments) dokumentech, konkrétně u protokolu http v dokumentu RFC 2616. [25] Http či https protokoly fungují na klasickém principu http request a http response, kdy se klient typicky pomocí webového prohlížeče dotáže na webový server, který určitým způsobem reaguje. Reaguje zpravidla tak, že odesílá danou webovou stránku. Po provedení takovéto komunikace je spojení mezi klientem a serverem ukončeno. Toto celé probíhá bez nutnosti znalosti, odkud se daný klient na zdroj dotazuje. Z pohledu serveru nemusí být poznat, zda dva po sobě jdoucí požadavky mají spolu souvislost či nikoli, http protokol tyto souvislosti jednoduše neřeší. Z tohoto důvodu se http a https protokolům říká bezstavové protokoly. Celý proces komunikace nejlépe vystihuje následující obrázek ze serveru ntu.edu.sg. [26]



Obrázek 2 – Komunikace http zdroj: ntu.edu.sg [26]

Na obrázku je možné vidět schéma již popsané komunikace. Zde je možné si všimnout bezpečnostního rizika při komunikaci mezi klientem a serverem, přičemž celá komunikace probíhá zcela nechráněná, takzvaně v „plain textu“ v nezašifrované formě, což je v mnoha případech velký bezpečnostní problém. Tento problém je zásadní především při komunikaci citlivých systémů, jako jsou například bankovní systémy, autorizační služby, různé portály na sjednání pojištění po internetu a kterékoliv jiné aplikace, které operují s citlivými daty či hesly. V případě, že by se útočník dostal k dané komunikaci například odposlechnutím (MITM útok) či jinou cestou, měl by k dispozici veškerá přenášená data, což by v některých případech mohlo znamenat únik velkého množství velice citlivých údajů. Toto riziko umocňuje i fakt, že protokol http nepoužívá žádný kontrolní součet ani jinou metodu ochrany zachování integrity dat během přenosu. To může reálně znamenat, že pokud útočník kontroluje alespoň jeden z bodů, po kterém komunikace probíhá, je schopen data v komunikaci změnit. Například útokem nazývajícím se „active attack“. [27]

2.8.1. HTTPS

Výše zmíněný bezpečnostní problém částečně řeší protokol https, který k protokolu http přidává koncové písmeno „s“, jež má význam klíčového slovíčka „secure“ (Hypertext Transfer Protocol Secure). Https protokol šifruje komunikaci mezi klientem a serverem pomocí TLS protokolu (Transport Layer Security), případně pomocí jeho předchůdce SSL (Secure Sockets Layer).

Dle společnosti Google [28] jsou označovány tři hlavní bezpečností vrstvy https protokolu, je to šifrování, integrita dat a ověření.

Šifrování: Https šifruje přenášená data, čímž je chrání před odposlechnutím ze strany útočníka. To znamená, že nikdo nemůže odposlouchávat danou konverzaci, případně sledovat aktivitu na stránkách ani jinak ukrást jakékoliv použitelné údaje během komunikace.

Integrita dat: Pomocí sofistikovaných metod je zamezeno možnosti změny či jiné formy manipulace s daty, aniž by to nebylo zjištěno.

Ověření: Poskytuje potvrzení, že uživatelé opravdu komunikují s požadovaným webovým serverem. Poskytuje ochranu proti útokům typu man-in-the-middle a posiluje důvěru uživatelů v daný server.

Dříve se https protokol používal převážně jen jako bezpečnostní faktor u online plateb. Avšak s postupným rozvojem internetu se https zabezpečení začalo používat i mimo platební segment. Dnes je použití https protokolu zcela běžné, ba i dokonce žádoucí. Oficiální vyjádření společnosti Google k protokolu https zní, že je třeba chránit každý web https protokolem bez ohledu na jeho obsah. [28]

2.8.2. TLS

Jak již bylo řečeno, k zabezpečení https protokolu se používá kryptografický protokol TLS, případně jeho předchůdce SSL. Cílem protokolu TLS je především poskytovat soukromí a integritu dat mezi dvěma nebo více komunikujícími. Různé verze TLS protokolu mají široké uplatnění hlavně ve službách jako například web browsing, email a instant messaging. [29], [30]

K samotné bezpečnosti TLS protokolu přispívá i fakt že certifikát, který server odesílá, vystavuje takzvaná Certifikační autorita. Certifikační autorita je subjekt, který spravuje a vydává digitální certifikáty, přičemž zároveň potvrzuje pravost informací v nich uvedených, čímž dopomáhá k využívání infrastruktury veřejného klíče (PKI – public key infrastructure). Tato infrastruktura má za následek to, že pokud klient obdrží platný certifikát, může si být jistý tím, že komunikuje právě se serverem, který je uveden v daném certifikátu.

Co je důležité o TSL protokolu říct na konec, je fakt, že pracuje pod vrstvou http protokolu. Pokud bude brán v potaz klasický ISO/OSI model, který obsahuje sedm

vrstev, dle serveru wordference.com [31] protokol https kombinuje vrstvy pět, šest a sedm na rozdíl od klasického http, který pracuje pouze na sedmé vrstvě, aplikační vrstvě ISO/OSI modelu. S tímto souvisí i skutečnost, že https protokol nepoužívá klasicky port 80, který je charakteristický pro protokol http, ale svůj port 443.

2.9. Virtualizace

Žijeme v době, ve které se informační systémy vyvíjejí neuvěřitelnou rychlostí. Téměř každý člověk žijící v moderním světě slyšel o společnostech, jako jsou například Facebook, Twitter či Google. Tyto společnosti jsou opravdovými giganty ve své třídě, u kterých si asi každý dovede představit, jaké hlavní služby nabízejí. Kvalita, rychlost, efektivita či dostupnost těchto služeb je přitom na extrémní úrovni. Stejnou úroveň musí mít na pozadí také infrastruktura dovolující provozování těchto služeb. Jedna z technologií, která výrazně usnadňuje provoz a růst těchto služeb, se nazývá virtualizace.

2.9.1. Proč virtualizovat

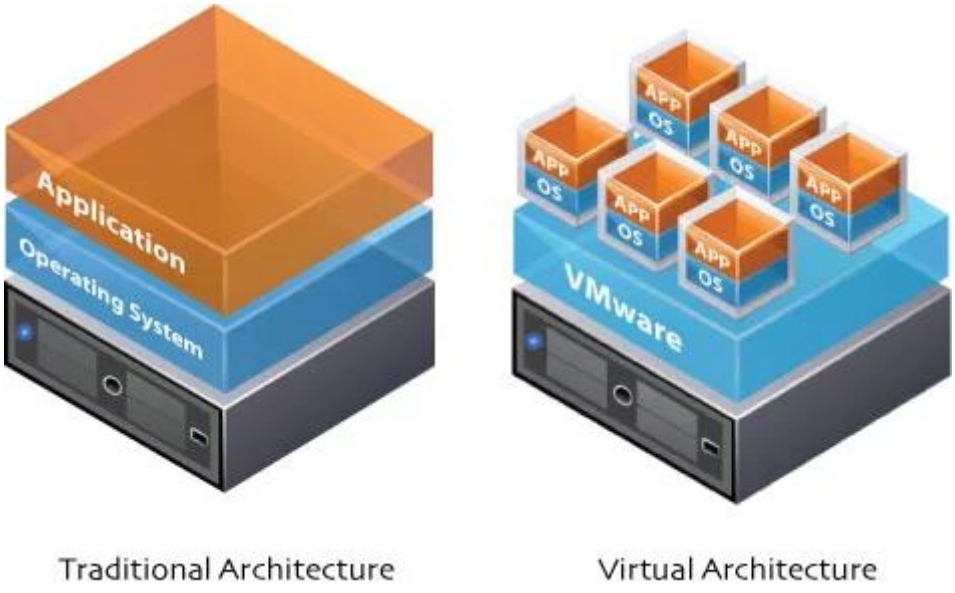
Jako první velice specifický důvod pro tuto práci předtím, než budou předneseny všeobecné důvody, proč nasazovat do virtualizovaného prostředí, je třeba si uvědomit, že veškeré systémy v ZF Frýdlant jsou nasazeny na virtualizovaných operačních systémech. Tudíž není důvod porušovat pravidlo stavěním specifického hardwaru. Oproti snadnému vytvoření virtuálního stroje. Proto i v této práci budou veškeré systémy nasazeny do virtualizovaného prostředí.

Jak říká Charles David Graziano [32], vznik a velké rozšíření virtualizace je částečně způsobeno velkým nárůstem hardwarového výkonu, který se za poslední desetiletí přinejmenším zdesetinásobil. Dále pak snahou snížit náklady na provoz v datových a IT centrech. Coby hlavní komplexní cíl virtualizace lze určit snahu o minimalizaci fyzického hardwaru potřebného k realizaci a následné údržbě veškerých IT systémů. Doba, kdy měl každý server vyhrazený svůj specifický hardware, aby nedocházelo ke konfliktu jednotlivých aplikací, je již dávno pryč. Tento způsob využití hardwaru byl vysoce nehospodárný, přičemž docházelo ke zbytečnému plýtvání zdroji a výpočetním výkonem. Většina takovýchto serverů nevyužívala ani zdaleka svůj maximální výpočetní výkon. [33]

Pomocí virtualizace lze tento výkon efektivně distribuovat mezi všechny nasazené aplikace. Pokud například máme na jednom fyzickém hardwaru, který může reprezentovat jeden výkonný server, hned několik slabších virtuálních strojů, tyto virtuální stroje pak disponují samozřejmě o něco menším výpočetním výkonem než celý server, avšak zpravidla jsou na většinu potřebných úloh, pro které jsou určeny dostačující. Tímto lze distribuovat jeden výkonný hardware na více nenáročných úloh, což je výrazně efektivnější než na každou úlohu nasazovat jeden slabší hardware.

Co je nutné zmínit k výkonu u virtualizace je to, že samotná virtualizace a její režie sebere určitý díl výkonu. Jak velký díl výkonu to bude, záleží převážně na typu virtualizace a charakteristice nasazených úloh. Jako zajímavost lze uvést, že u určitého druhu virtualizace lze docílit i toho, že všechny virtuální stroje dohromady mohou mít větší paměť nebo více procesorových jader nežli skutečný hardware, na kterém běží.

Pro lepší představu kontrastu a následné pochopení virtualizace oproti tradičnímu přístupu lze využít obrázek z webu redswitches.com [34], který vypadá následovně.



Obrázek 3 – Typy architektury zdroj redswitches.com [34]

Na obrázku lze vidět architekturou takzvané para virtualizace s nativním či bare-metal hypervisorem. Tento typ virtualizace je často používaný pro žádanou serverovou virtualizaci. Daný typ virtualizace se svými specifiky je popsán dále. Jak je

možné vidět na obrázku, virtualizace kromě běhu mnoha různých prostředí zajišťuje ještě jednu důležitou věc, A to separaci daných prostředí.

Virtualizace tedy poskytuje možnost běhu mnoha různých prostředí vedle sebe, ať už se jedná o virtualizaci celých operačních systému či takzvanou kontejnerizaci. Tato technologie umožnuje nasazení jinak nekompatibilních aplikací na jeden sdílený hardware. Například pokud existuje již zmíněný jeden výkonný server, který má obsluhovat dvě méně náročné aplikace. Tyto aplikace může reprezentovat například e-shop a zároveň aplikace spravující skladové hospodářství přidružená k tomuto e-shopu. Každou aplikaci musí spravovat jiný správce, který žádá jiné běhové prostředí (například Windows/Linux, x86/x64). Dochází tak ke konfliktu, kdy určité aplikace nelze provozovat paralelně vedle sebe v jednom prostředí. Nelze hovořit pouze o konfliktu v konfiguraci či prostředí, ale o celkové obtížnosti poskytnout jeden server s jedním běhovým prostředím pro více úloh.

Samozřejmě klasickým přístupem tento problém lze taktéž řešit, a to postavením více slabších serverů, na kterých budou nasazeny jednotlivé úlohy. Avšak tento způsob je dosti krkolomný (mnoho redundantních částí oproti jednomu silnému serveru), navíc dostačující je pouze do doby, kdy je zapotřebí určitá míra rozšiřitelnosti a škálovatelnosti. Jednoduchým příkladem může být již zmíněný rozrůstající se e-shop, který potřebuje zvýšit výpočetní výkon pro rychlou obsluhu všech svých zákazníků. Pokud daný e-shop bude nasazen na slabém serveru, zpravidla toto rozšíření bude znamenat nutnost vylepšení serveru či v horším případě pořízení celého nového či dalšího stroje. Naopak pokud bude nasazen na dostatečně silném virtualizovaném stroji, znamená to pouze přidělení danému stroji více hardwarových prostředků (pokud jsou k dispozici, případně lze omezit ostatní běžící služby na daném stroji), což lze udělat pár kliknutími v konzoli pro správu.

S tímto úzce souvisí přenositelnost a určitá míra zálohování systému. U přenositelnosti systému, pokud bude e-shop nasazen přímo na jakémkoli hardwaru, ta bude na takové úrovni, že přesun na jiný hardware bude znamenat znovu projít kompletní proces nasazení včetně instalace samotného prostředí a následné migrace veškerých dat. To v určitých případech může být velmi náročná operace, která se neobejde bez odstávky daného serveru. Oproti tomu bude-li daný

e-shop nasazen ve virtualizovaném prostředí, proces migrace znamená pouze nutnost nasazení na nový hardware dané virtualizační prostředí a jednoduché přenesení virtuálních strojů, což například v nástroji VMware ESXI lze udělat exportem do takzvaného souboru OVF a následným importem do daného prostředí, čímž se systém přenese téměř bez toho, aniž by do něj bylo jakkoliv zasaženo.

Věc, kterou je třeba neopomíjet, je zálohování neboli, jak rčení praví, IT administrátoři se dělí pouze na dva typy lidí, ty, co zálohují, a ty, co budou zálohovat. Skutečnou sílu a vážnost, se kterou by se mělo k zálohování přistupovat, lze totiž pochopit až potom, co jsou data ztracena. Dnes už si lze jen těžko představit CIO (Chief information officer), který by na sebe vzal tak velkou zodpovědnost a nechal své systémy bez zálohy. Zde správcům daného systému opět virtualizace poskytuje určité zjednodušení. V konkrétních virtualizačních nástrojích lze mimo jiné nastavit pravidelné zálohování pomocí takzvaných snapshotů, které poskytují vcelku rychlou a efektivní možnost zálohování. Avšak je nutné nezapomínat, že snapshoty nejsou samospasné a nesou s sebou i jistá omezení, která jsou zmíněna dále.

Oproti tomu zálohování systému, který je nasazen přímo na fyzickém hardwaru, je ještě problematičtější. Samozřejmě lze vytvářet bitové kopie například celého disku, avšak takovýto způsob je časově náročný a vytvořenou bitovou kopii lze znovu použít jen na velmi podobném nebo nejlépe totožném hardwaru. Existuje i mnoho dalších způsobů, než jenom vytváření bitové kopie, jak lze zálohovat určité prostředí, avšak virtualizační nástroje posouvají možnosti zálohování ještě o stupínek výše. Před uvedením typu a rozdělení virtualizace by bylo vhodné určité shrnutí a objektivní zhodnocení virtualizace jako celku. To lze udělat jednoduše pomocí jejich všeobecných kladů a záporů.

2.9.2. Výhody a nevýhody virtualizace

Každý typ virtualizace s sebou pochopitelně nese své konkrétní výhody a nevýhody. Přesto virtualizace jako taková má všeobecná pro a proti. K přehlednému srovnání těch nejdůležitějších postačí jednoduchá tabulka, která může vypadat následovně. [35]–[37]

Výhody	Nevýhody
Sdílení zdrojů	Režie snižující výkon
Separace	Single point of failure
Snížení nákladů	Nárůst složitosti
Přenositelnost / Migrace	

Toto není zdaleka výčet všech kladů a záporu virtualizace, avšak postačí pro jasnou představu, k čemu tuto technologii lze využít a kde jsou její silné a slabé stránky. Určité nevýhody lze v praxi více či méně potlačit tak, aby byly zanedbatelné, či jejich dopad se výrazně snížil. Příkladem může být disaster recovery plán pro určité zařízení, které reprezentuje single point of failure.

Před použitím samotné virtualizace je třeba objasnit několik dalších věcí. Praktické využití se však odvíjí od použitého typu virtualizace. Typů, jak je možné určité systémy či jeho části virtualizovat, je přitom hned několik.

2.10. Hypervisor a jeho typy

Jelikož dnes kromě operačních systémů lze virtualizovat mnohé, například sítě, úložiště ale i paměť, je důvodem, proč se i pohledy na rozdělení virtualizace častokrát z odlišných zdrojů poněkud liší. Různě je uváděno rozdělení od desktopové virtualizace až po síťovou [38] či od OS (myšleno operační systém) virtualizace až pro Storage virtualizaci. [39] Nebo například od emulace, kdy se virtualizuje úplně všechno včetně hardwaru, až po kontejnerizaci, kdy se od sebe oddělují pouze běžící aplikace v určitém prostředí. Jelikož v této práci je třeba virtualizovat výhradně serverový operační systém, není rozdělení virtualizace až tak podstatné. Je vhodné zmínit pouze jeden typ, a to hardwarovou virtualizaci, která je důkladněji zmíněná na serveru redswitches.com. [34] Hardwarová virtualizace je v oblasti virtualizování serveru tou nejrozšířenější. Konkrétně tedy ne celá hardwarová virtualizace, ale pouze jeden její podtyp či dalo by se říci metoda, a to virtualizace za pomocí hypervisoru.

Na začátek je pro pochopení třeba objasnit, co to hypervisor je a jaké jsou jeho funkce. Bernard Golden ve své knize [35] popisuje přesný význam a princip vzniku slova

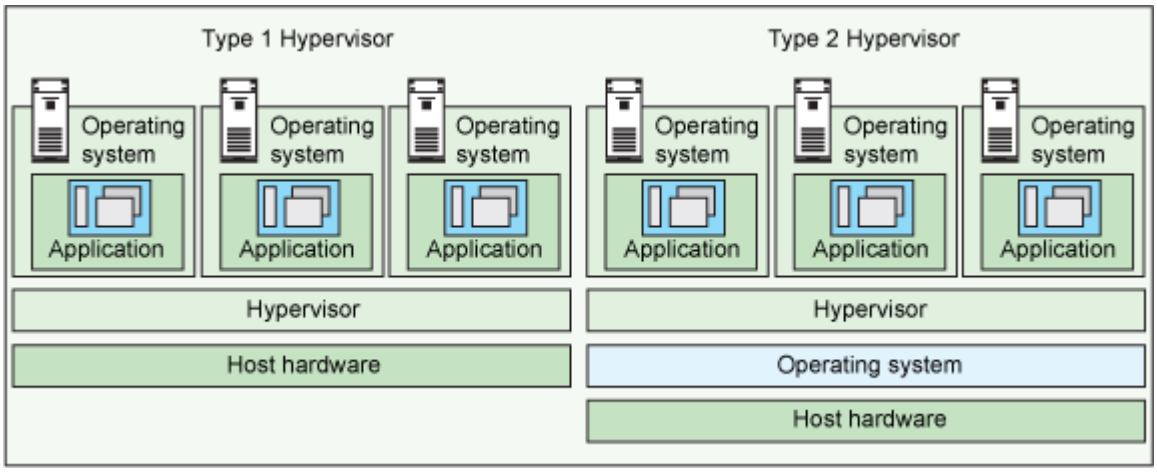
hypervisor jako jakési hraní si se slovy. Tím, že operační systém je občas nazývaný jako supervisor či český ekvivalent dozorce a pokud při virtualizaci existuje jiný určitý software v podobě supervisora, který dohlíží na ostatní operační systémy (supervisory), je tento software supervizorem supervizorů neboli hypervisorem.

Existuje spousta vznešených definic, co to hypervisor je. Avšak k pochopení významu postačí jednoduchý příklad. Před několika lety jeden nejmenovaný učeň v ZF Frýdlant měl o serverové virtualizaci pouze mlhavá tušení. Kolega, který ho v tu dobu zaučoval, pojem hypervisora vysvětlil následující, sice jednoduchou, ale velice hezkou definicí. Pokud existuje klasický počítač jako celek s normálním operačním systémem, je několik zásadních věcí, o kterých daný operační systému musí určitým způsobem vědět. Jako například je-li připojená nějaká klávesnice, myš, monitor, zda jsou zde nějaké ovladače a spousta dalších věcí, jako jsou například USB porty, mechaniky, ale i informace, jako například kolik je dostupné operační paměti, jaký procesor s kolika jádry aj. Všechny tyto věci vyplývají zpravidla z hardwaru, ovšem pokud operační systém neběží na hardwaru ale v jakémsi virtuálním prostředí, kde všechny tyto věci jako klávesnice, myš a tak dále nejsou, je třeba danému operačnímu sytému tyto věci pouze určitou formou zprostředkovat. Je důležité, aby daný operační systém věřil, že všechna tato zařízení jsou k dispozici. Jinými slovy je třeba tyto věci virtualizovat či tak zvaně lhát operačnímu systému o těchto věcech. Toto je přesně úloha, kterou zastává software zvaný hypervisor. Hypervisor je software, který emuluje již zmíněné části počítače pro operační systémy. Nadneseně by se dalo říci, že hypervisor vytváří prostředí pro operační systém tak, aby si myslel, že běží na reálném hardwaru.

Firma Red Hat je společností poskytující jednu z nejznámějších distribucí Linuxu a taktéž zabývající se virtualizací, cloud computingem a jinými softwarovými nástroji. Na jejich stránkách je souhrnně řečeno [40], že hypervisor je software, který vytváří, spouští a řídí virtuální stroje. Hypervisor někdy nazývaný jako VMM (virtual machine monitor) izoluje operační systémy a jejich zdroje. Ačkoli to nemusí být na první pohled jasné. Všichni hypervizoři potřebují určité komponenty, se kterými pracují klasické operační systémy, jako jsou například správce paměti, plánovač procesů, zásobník, ovládače a tak dále. Společnost Red Hat zmiňuje to, že klíčová vlastnost virtualizace je možnost běhu více operačních systémů, které sdílí jeden hardware.

Následně jako zajímavost lze uvést, že v textu je hypervisor VMware ESXi zmíněn jako velice populární nástroj pro virtualizaci.

Jak je možné zjistit již na uvedených stránkách společnosti Red Hat [40], existují dva typy hypervisorů, a to velice prozíravě nazvané hypervisor typu 1 a typu 2. Hypervisor typu 1 někdy také nazývaný nativní či „bare metal" hypervisor [41] běží přímo na daném hardwaru, kde spravuje dané operační systémy. Oproti tomu hypervisor typu 2 běží podobně jako jakákoliv jiná aplikace na již spuštěném operačním systému a poskytuje určité rozhraní, přes které je možné vytvořit VM (Virtual machine). Typy hypervisorů nejlépe zobrazuje obrázek z již zmíněného webu VapourApps. [41]



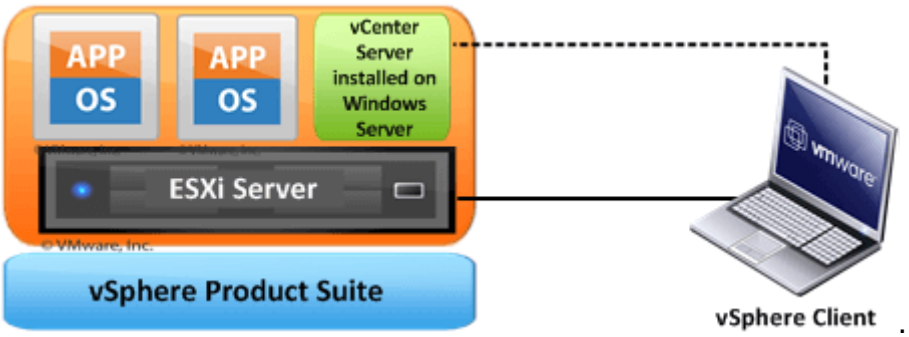
Obrázek 4 – Typy hypervisorů zdroj: VapourApps [41]

Dle obrázku mezi Hypervisorem typu 1 a 2 je jediný rozdíl, a to mezi přidanou vrstvou operačního systému u hypervisoru typu 2, avšak tato vrstva muže dosti ovlivňovat výkon a stabilitu celého systému. Tomuto napovídá i fakt, že VMware ESXi, který je jedním ze zástupců hypervisora typu 1, je v článku Performance analysis of selected hypervisors téměř nejlépe hodnoceným hypervisorem z hlediska výkonu. [42] Je zde zmíněn i důvod výpočetní převahy hypervisora typu 1, a to díky přímému přístupu k hardwaru, který hypervisor typu 2 nemá. Oproti tomu například Virtualbox, který je typickým zástupcem hypervisora typu 2, dopadl v určitých testech velice obstojně, viz zmíněný článek. [42] Ukázalo se, že pokles výkonu v určitých operacích nemusí být tak rapidní, jak by se dalo čekat, avšak daný pokles výkonu se odvíjí zpravidla od druhu vykonávané úlohy.

Jako poslední věc k hypervisorům je vhodné zmínit některé z řad jejich zástupců. Jako hypervisora typu 1 lze uvést již zmiňovaný, hojně používaný VMware ESXI a dále například Microsoft Hyper-V nebo Citrix XenServer, který je částečně open-source pod licencí GPLv2. K hypervisoru typu 2 lze jako hlavní hráče uvést Virtualbox od společnosti Oracle a VMware workstation player jako jeho hlavního konkurenta. Do třetice pro hypervisora typu 2 je možné zmínit ryze linuxovou záležitost, a to nástroj KVM, který je sice o něco složitější jak ke konfiguraci, tak k použití, avšak o to víc možností nabízí.

2.11. VMware vSphere

Ještě před podrobnějším pohledem na samotný VMware je vhodné představit tak zvaný vSphere. Zde může existovat spousta otázek, co je to přesně vSphere, ESXI a například vCenter a jaký je mezi nimi vztah. Nejen mezi širokou veřejností, ale i v komunitě správců často dochází k záměně či překryvu těchto výrazů, a to kvůli nepřesné či mlhavé znalosti vztahů mezi nimi. Vzájemné vztahy mezi vSphere, ESXi a vSphere klientem nejlépe zachycuje obrázek z webu mustbegeek.com. [43]



Obrázek 5 – vSphere balík zdroj: mustbygeek.com [43]

Jak je možné poznat z obrázku a je i řečeno v přidruženém článku [43], vSphere je v podstatě souhrnný balík, který sdružuje nástroje jako ESXi, vSphere klient a další. Pro lepší představu lze uvést analogii, například existující u balíčku MS office, kdy tento balíček zahrnuje mnoho komponent jako například Word, Excel a tak dále. Tyto komponenty společně tvoří jeden ucelený balík a stejně jako u vSphere nesou jeden souhrnný název, za nímž následuje název komponenty.

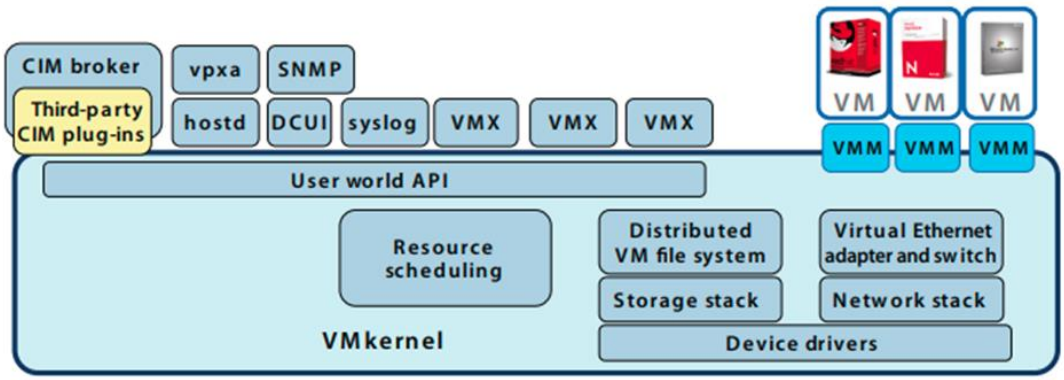
U balíčku MS office to nelze přesně určit, avšak u vSphere by se za nejdůležitější komponentu balíčku dal označit ESXi server. Veškeré virtuální stroje jsou nainstalovány právě na ESXi serveru. Pro správu těchto virtuálních strojů lze využít

dalšího nástroje z balíčku vSphere, a to vSphere klienta, který muže být reprezentován pouze klasickým webovým rozhraním. Klient a samotné webové rozhraní je zmíněno dále, avšak jak již bylo řečeno výše, nedůležitější částí zůstává ESXi.

2.11.1.1. VMware ESXi

Hned na začátku je důležité zmínit jednu z největších výhod VMware ESXi (nebo dále jen ESXi). Jak tvrdí článek na webu computerworld.com [44], VMware jako hypervisor má dlouhodobě dominantní postavení na trhu. To znamená, že je pro něj optimalizováno mnoho aplikací důležitých pro podnikovou sféru, jako jsou například databáze Oracle, MS SQL Server a další, což hraje velkou roli při výběru virtualizačního nástroje k budování podnikové infrastruktury. Jelikož do podnikového prostředí nelze nasazovat neprověřené, dokonce neprofesionální klíčové nástroje, právě z toho důvod byl pro tuto práci vybrán nástroj VMware ESXi.

ESXi je tedy hypervisor typu 1. To znamená, že se nejedná o nainstalovanou aplikaci v operačním systému, ale je to takzvaná „bare metal" virtualizace [45], kdy je hypervisor nainstalován přímo na fyzický hardware. Je vhodné uvést, že samotný hypervisor je s určitým nadhledem minimalizovaným operačním systémem se všemi náležitostmi, jako je například multitasking či tak zvané swapování a tak dále. Při práci s ESXi se může zdát, že se jedná o linuxové jádro. Avšak není tomu tak, jedná se o jádro nazvané VMkernel. [46] VMkernel je platforma zvaná microkernel-based [47] neboli platforma založená na mikrojádru, které je optimalizované speciálně pro účely virtualizace. Samotné jádro vypadá následovně.



Obrázek 6 – Jádro VMkernel zdroj: The Architecture of VMware ESXi [46]

Jak lze vidět, jádro obsahuje několik komponent například pro plánování zdrojů, distribuci VM souborového systému, virtuální ethernetový adaptér včetně virtuálního switche a další. Jádro poskytuje určité funkce podobné těm, které lze nalézt i v jiných operačních systémech, jako jsou například zásobníky I/O, signály, správa paměti a tak dále. Je vhodné si všimnout, že jádro obsahuje ovladače k hardwaru, což je podstatné, jelikož i z tohoto důvodu nelze nainstalovat VMware ESXi na každý hardware, ale pouze na určité typy hardwaru, které výrobce podporuje a má zakomponované v daném jádře.

VMkrenel je kromě již řečených klasických operací, které lze nalézt i v jiných jádrech, zodpovědný za implementaci hardwarových specifik a následné odstínění virtuálních strojů od těchto specifik, a to pomocí vytvoření hardwarové abstraktní vrstvy pro virtuální stroje. [48] Pomocí této vrstvy server ESXi vytváří přenosné virtuální stroje, které nejsou jako klasické počítače závislé na hardwaru. S přenosem virtuálních strojů úzce souvisí formát exportu a importu jednotlivých strojů, který bude zmíněn dále.

Před praktickou částí práce je vhodné doplnit pár zbývajících pojmů a technologií, na které je možné ať už v praktické části práce či při hlubším zkoumání daného oboru narazit.

2.11.1.2. OVF / OVA

Někdo by mohl říci, že doposud zmiňované, nepřesně avšak v praxi často používané označení OVF (slangově řečeno OVFko) neboli open virtualization format je zavádějící. Jelikož při exportování virtuálního stroje, hypervisor vytváří zpravidla OVA soubor, tento fakt je vhodné objasnit. OVF je otevřený standard pro balení a následnou distribuci softwaru pro virtualizaci. [49] Oproti tomu OVA neboli open virtual appliance či application [50] je, velice abstraktně řečeno, jiný název pro stejnou či velice podobnou záležitost. Jedná se o soubor, který vzniká určitým procesem. Jedná se o proces jakéhosi zabalení zpravidla jednoho virtuálního stroje se všemi jeho aplikacemi, softwarem a závislostmi. Virtuální stroj se zabalí do jednoho balíku a následně vyexportuje do souboru s koncovkou OVF či OVA. Rozdíl v těchto dvou souborech je pouze ten, že OVF je adresář s více soubory, oproti tomu OVA je

jeden velký zabalený (zpravidla do tar) soubor, který obsahuje mimo jiné i soubor OVF. Ve zkratce je tedy OVF složka se soubory, OVA je vše v jednom. [51]

2.11.1.3. Snapshot a zálohování

Snapshot, jak již bylo řečeno, úzce souvisí se zálohováním a případným obnovením dat ze zálohy, tedy s disaster recovery plány. To platí, ať už se jedná o zálohu jednoduchých dat, jako jsou například textové či multimediální soubory, nebo o zálohu komplexních operačních systémů se všemi soubory, vazbami či zaváděcími a jinými částmi disku. Jelikož je zde v práci snapshot zmiňovaný spíše jako možnost pro zálohy virtuálních strojů, bude i zde popisován obzvláště z pohledu zálohy virtuálních strojů za pomocí hypervisora.

Jak je zmíněno na stránkách systemonline.cz, [52] které byly jedním ze zdrojů následující kapitoly, před rozmachem virtualizace, kdy ke každému operačnímu systému připadal jeden fyzický hardware, implementovala se zálohovací řešení na úrovni operačního systému. Tehdy se do operačního systému nainstaloval určitý agent, který manipuloval a dále spravoval veškerá data, která byla potřeba zálohovat. Avšak tento přístup zcela změnil příchod virtualizace. Pokud by došlo k nasazení takového agenta na každý virtuální stroj, v řádu desítek až stovek virtuálních strojů se tento agent se všemi svými režijními požadavky (síť, CPU, RAM) stává velice neefektivní. Virtualizace nabízí řešení tohoto problému v podobě centralizované správy těchto procesů bez nutnosti instalace klienta, pouze za pomocí hypervisora. V tomto kontextu vznikly tak zvané snapshoty neboli kopie disku virtuálního stroje zpravidla ve formátu VMDK v určitém čase. [53] Snapshot obvykle dokonale zachytí stav virtuálního stroje, který uloží pro případné budoucí použití ve formě obnovy tohoto stavu. Jak říká Petra Šváb v již zmíněném článku, snapshoty samy, případně s příspěvkem dalších technologií, při obnově pomáhají jak k minimalizaci RTO (Recovery Time Objective), tak ke snížení stáří RPO (Recovery Point Objective).

Avšak je nutné zmínit i zápory zálohování pomocí snapshotu, jelikož dlouhodobé uchovávání snapshotů z důvodu jejich velikosti může být velice nákladné. Snapshoty dobře poslouží při požadavku krátkodobé retence dat, jelikož poskytují nejrychlejší možnost zálohování, avšak zabírají mnoho diskového místa. Z hlediska dlouhodobé

retence dat existují řešení založená například na magnetických páskách, externích jednotkách či jiných zařízeních k tomu určených.

Závěrem ke snapshotům je vhodné poznamenat, že poskytují velice zajímavé a efektivní možnosti zálohování, avšak tato technologie má sama o sobě určité nedostatky, které lze eliminovat například kombinací s jiným typem zálohování. Následně se z této technologie stává velice užitečný pomocník při ochraně dat. A to hlavně z důvodu rychlosti a efektivity jak obnovy, tak zálohy dat.

3. Implementace

V této kapitole bude podrobně popsáno praktické nasazení softwaru pro centralizovaný IT management Symantec Altiris včetně veškerých potřebných doplňkových nástrojů, požadavků a implementačního serveru. Dále zde bude popsána a provedena instalace softwaru pro serverovou virtualizaci, a to softwaru VMware esxi ve verzi 6.7.0. tak, jak probíhala v ZF Frýdlant.

3.1.1. VMware esxi

Jako první krok pro instalaci VMware ESXi je třeba zkontrolovat, zda daný hardware, na který bude nainstalován, splňuje minimální požadavky pro běh daného systému. Veškeré požadavky lze nalézt ve webové dokumentaci VMware docs. [54]

Je vhodné zde také zmínit alespoň výčtem ty nejdůležitější požadavky, které jsou klíčové pro běh VMware esxi.

3.1.2. Základní požadavky na HW pro běh VMware esxi

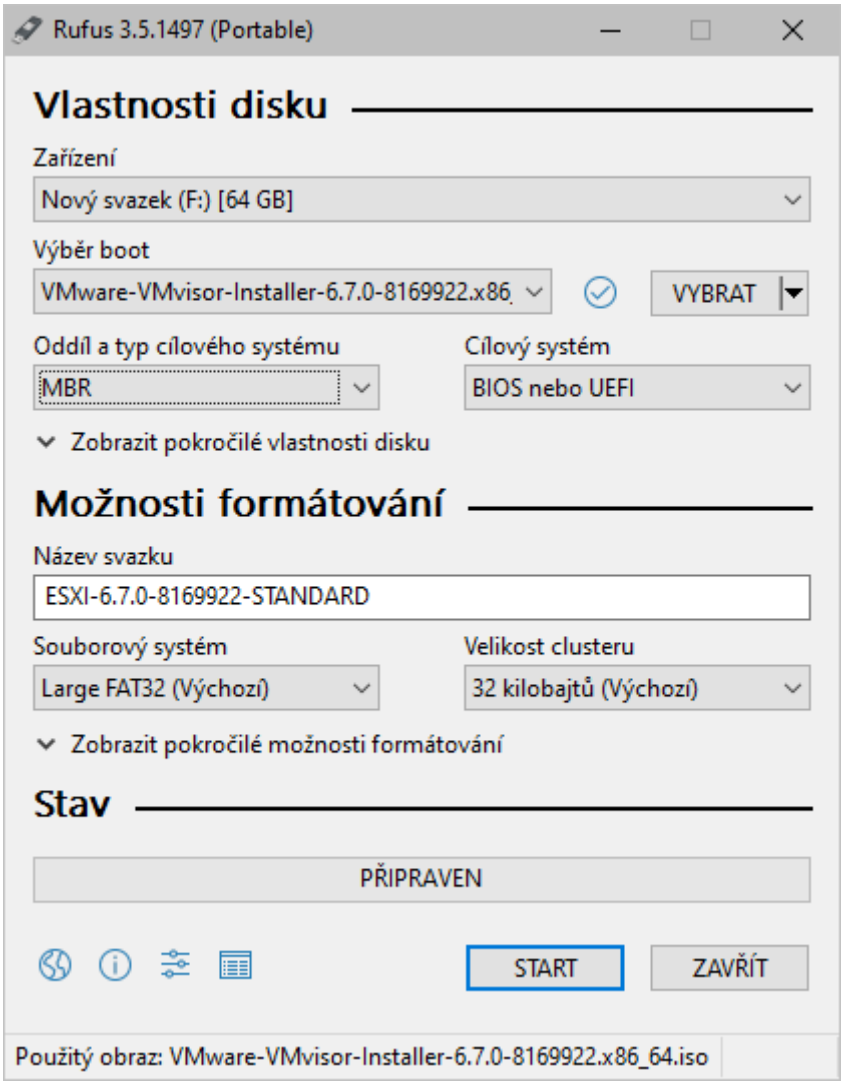
- Procesor s dvěma či více jádry.
- Minimálně 4 GB operační paměti (optimálně 8 GB a více).
- Intel VT-x nebo AMD RVI pro podporu 64x operačních systémů.
- Jednu či více ethernetových karet s rychlostí 1 GB/s nebo rychlejší.

Poté co proběhlo ověření, zda daný hardware splňuje požadavky pro nasazení daného systému, se lze uchýlit k dalšímu kroku, a to je stažení daného softwaru. Po registraci přímo na stránkách výrobce lze bezplatně stáhnout instalační ISO obraz VMware esxi zcela legálně přímo od něj. Na stejnojmenné stránce lze i bezplatně pouze pro ESXi získat licenční klíč. Bezplatná verze má však svá omezení, která jsou specifikována na daných stránkách. [55]

3.1.3. Vytvoření bootovacího média

Po dokončení stahování je třeba vytvořit zaváděcí médium, jako je DVD disk nebo ideálně USB flash disk. Při variantě vytváření USB lze na MS Windows vytvořit například open-source free nástrojem zvaným Rufus [56], případně Etcherem pro Linux či jakoukoliv jinou utilitou pro zapsání ISO obrazu na USB flash disk.

Pro tento konkrétní příklad nasazení bude použit již zmíněný nástroj RUFUS ve verzi 3.5.1497 portable. Jako médium bude použit flash disk značky Kingston o velikosti 64GB.



Obrázek 7 – Rufus bootable USB zdroj: vlastní

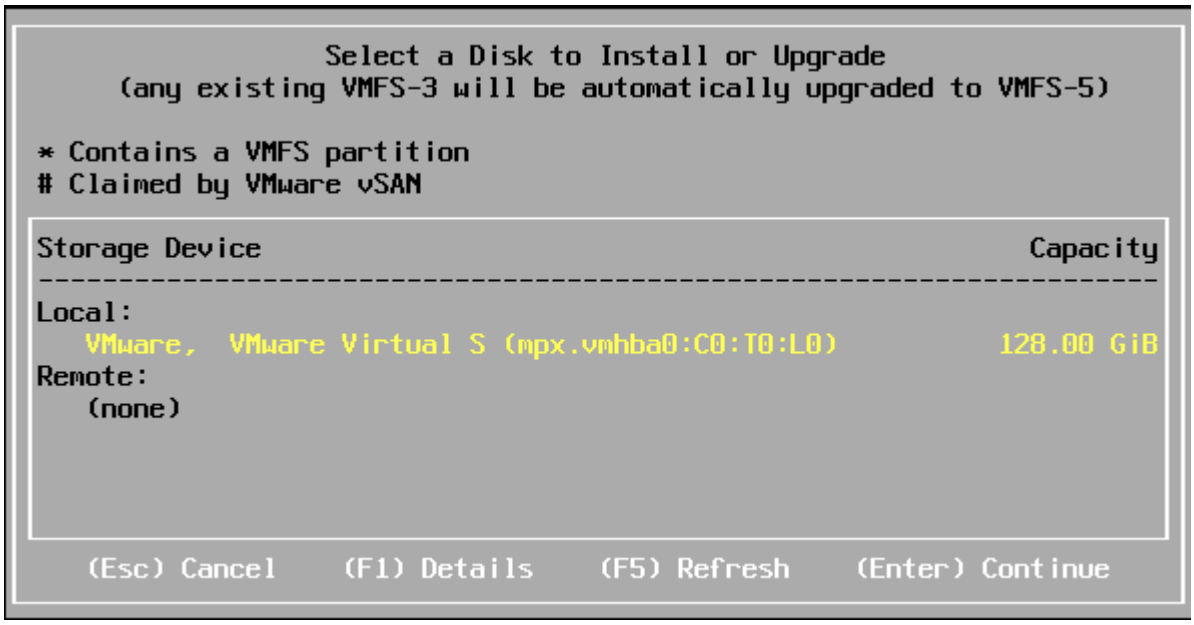
Nastavení vytváření nemusí být zcela zjevné, proto zde budou vysvětleny zásadní části konfigurace vytváření media. Jako první je zapotřebí vybrat USB zařízení, ze kterého má být vytvořeno zaváděcí medium. Následně vybrat samotný ISO obraz, pak vybrat typ oddílu MBR či GTP, které jsou zmíněný výše, a ostatní parametry mohou zůstat nezměněny ve výchozím nastavení. Nakonec zbývá už jen formálně pojmenovat medium a stisknout Start.

3.1.4. Instalace VMware ESXI

Po vytvoření bootovacího media je třeba ho připojit k sestavě, na které má ESXi běžet a nabootovat z daného media. Pro nabootování je třeba dostat se do bootovacího menu a zvolit dané zařízení. Do bootovacího menu se lze dostat klasicky při stisku vybrané klávesy při startu počítače.

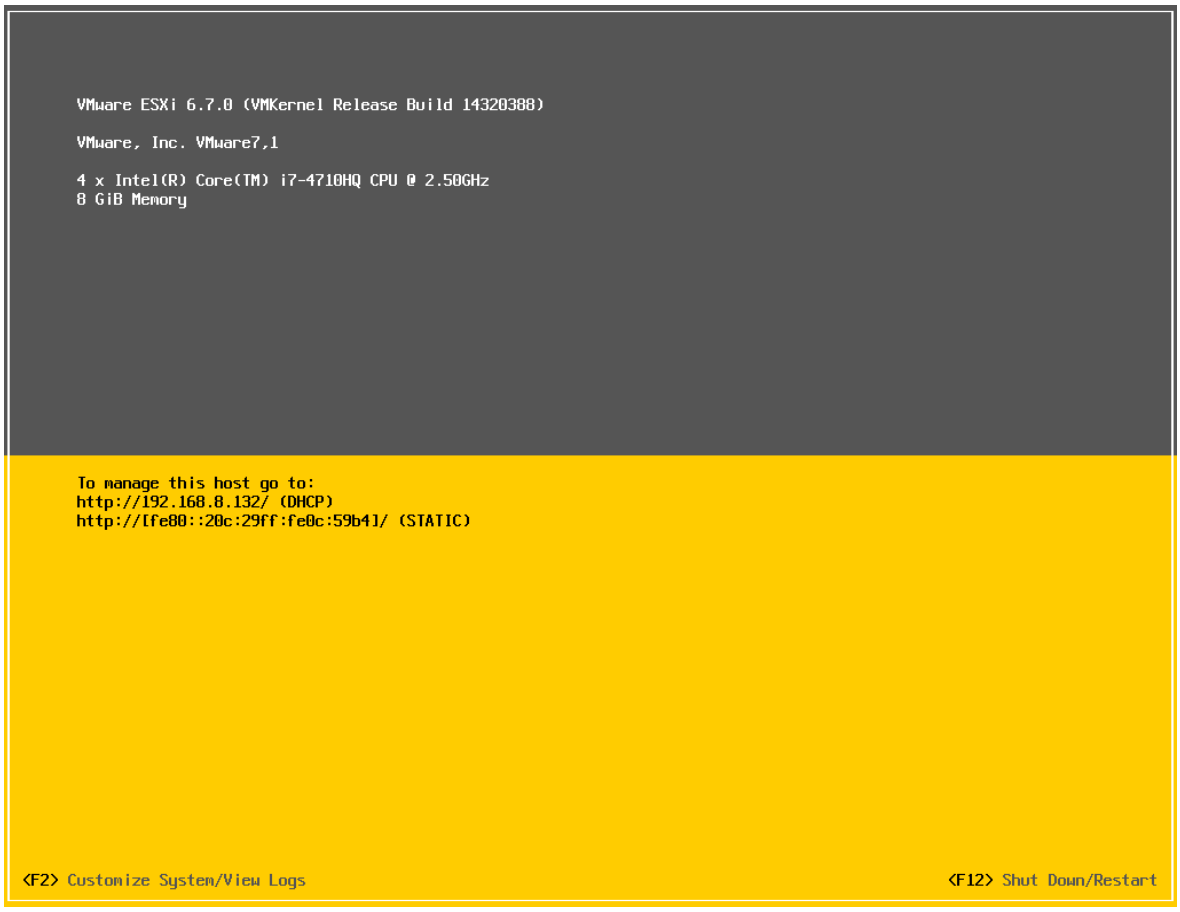
Po nabootování a načtení ESXI „installer“ (což může trvat pár minut) je potřeba odsouhlasit licenční podmínky a v některých případech kompatibilitu hardwaru. Následně je nutno vybrat disk, na který má být samotný VMware ESXi naistalován a potvrdit.

Výběr pro ukázku, průvodce vypadá následovně.



Obrázek 8 – Průvodce instalací ESXi zdroj: vlastní

Po potvrzení se instalátor postupně dotáže na rozložení klávesnice, heslo root uživatele a upozorní na to, že bude celý disk smazán. Po akceptování tohoto oznámení nastane samotná instalace, poté bude počítač restartován a měl by nastartovat do následujícího stavu.



Obrázek 9 – ESXi běžící systém zdroj: vlastní

Jak je možné vidět obrázku, systém po startu nenabídne příliš mnoho nástrojů pro práci, což by někoho mohlo zaskočit, avšak podstata tkví v tom, že se celý systém řídí z webového rozhraní, na které se dá přistoupit pomocí jedné z vypsaných adres. V tomto případě se jedná o adresu „192.168.8.132“ přidělenou DHCP serverem.

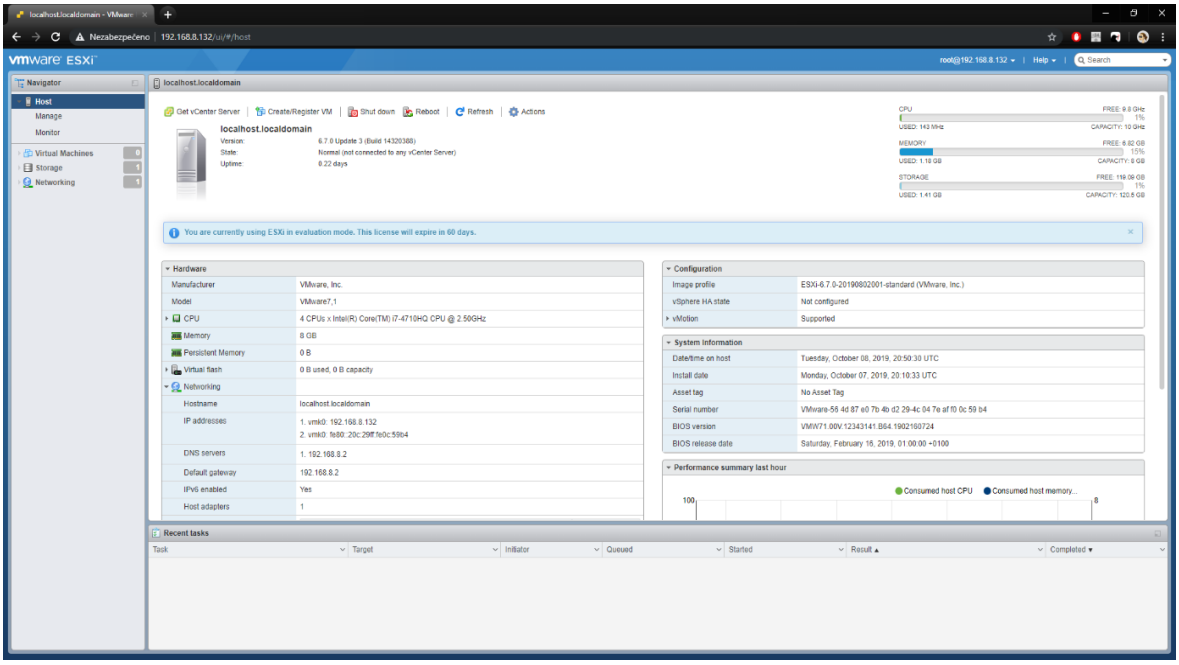
Poslední, co je před představením managementu systému vhodně zmínit alespoň zlehka, je skromná, avšak dostačující nabídka „customizace“ systému, která se skrývá pod klávesou F2.

Po stisku F2 a zadání hesla root uživatele se otevře menu, v němž je možné změnit heslo aktuálního uživatele, nastavovat a restartovat síťové připojení, určovat typ klávesnice a další. Co je tu však podstatné, jsou systémové logy. ESXi nabízí šest různých logů, výčtem to jsou {syslo, wmkernel, config, management agent (hostd), virtualCenter agent (vpxa), vmware esxi observation log (vobd)}. Jak už to u logu bývá, pokud by nastaly nějaké kritické problémy se systémem, je velká pravděpodobnost, že odpověď na příčinu bude tkvět právě v jednom z těchto logů.

3.1.5. Management VMware ESXI

Do webového prohlížeče je třeba zadat ip-adresu, která byla zmíněna dříve (zde konkrétně „192.168.8.132“), následně se objeví přihlašovací obrazovka, kde je potřeba vyplnit jméno (nejčastěji root) a heslo, které bylo zvoleno při instalaci systému. Je vhodné upozornit na to, že pokud je provedena opravdu čistá instalace, nebude s největší pravděpodobností zaveden SSL, případně TLS certifikát, což v důsledku znamená, že prohlížeč označí tuto stránku jako nedůvěryhodnou a zobrazí upozornění. Upozornění může vypadat v každém prohlížeči trochu jinak, avšak mívá většinou podobu varování „Vaše připojení není soukromé“. Zde není čeho se obávat, je zpravidla potřeba při prvním připojení otevřít další možnosti a vynutit přechod na danou stránku. Následně lze pro zvýšení bezpečnosti ve správě certifikátu daný certifikát dodat.

Po přihlášení se naskytne následující pohled.



Obrázek 10 – Správa VMware zdroj: vlastní

Přes toto webové rozhraní se řídí veškeré virtuální servery. Nachází se zde vše potřebné, od podrobného monitorování zdrojů jako procesor, paměť a další až po konfiguraci virtuálního switche, který je nezbytný pro celý proces virtualizace serverů. [57]

V tento moment již VMware ESXi plně běží a vše je připraven pro plnou virtualizaci serveru, na který bude nasazen samotný Altiris. Před nasazením operačního systému je vhodné zmínit volbu správy přes SSH, která lze v nastavení ESXi zapnout a následně podobně jako jiné linuxové servery spravovat daný nástroj přes SSH připojení.

3.2. Operační systém

Proto, aby mohl být implementován samotný „deployment solution system" je zapotřebí operačního systému, a to „serverového operačního systému“, který poskytne vhodné prostředí pro běh samotného Altirisu. Díky zpětné kompatibilitě, kterou společnost Microsoft drží u svých systémů, je možné Altiris nasadit na celou řadu vydání Windows serveru již od verze Windows server 2003. [58] V ZF Frýdlant je Altiris nasazen na Windows serveru verze 2016, tudíž zde bude ukázaná instalace stejné verze. Nicméně jednotlivé verze serveru jsou si velice podobné, pro obdobné verze by tedy byl následující postup téměř analogický. Jelikož některé kroky instalace mohou být nezajímavé, budou zde popsány pouze klíčové či neintuitivní momenty instalace nutné pro rozběhnutí serveru.

Jako první krok instalace je opět potřeba zkontrolovat minimální požadavky na hardware. Výčet těch nejzásadnějších může být následující.

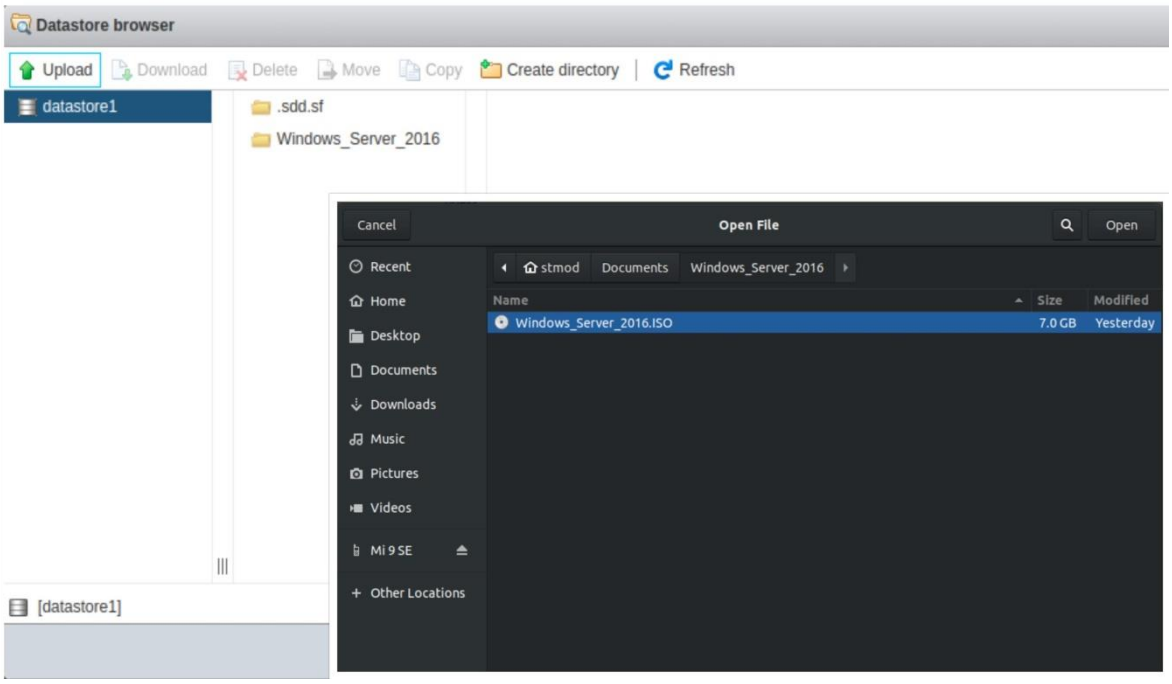
- Procesor podporující x64 architekturu.
- Alespoň 32 GB místa na disku.
- Minimálně 2 GB operační paměti pro podporu „Desktop Experience feature“.

Veškeré požadavky s podrobným popisem lze nalézt na stránkách docs.microsoft.com [59].

Poté již následuje samotná instalace. K té je třeba ISO soubor daného operačního systému, pro tento konkrétní případ ISO Windows server 2016. Lze jej bezplatně stáhnout například na oficiálních stránkách Microsoft (ač pouze trial verzi). [59] Je třeba pamatovat, že bezplatnou trial verzi lze užívat pouze po dobu 180 dní, poté je třeba zakoupit licenci k dalšímu užití.

Po stažení ISO souboru je třeba dané ISO nahrát do připraveného VMware ESXI. To lze udělat na záložce „Storage“, která obsahuje kartu s výchozím názvem „datastorage1“, jež slouží pro spravování přiděleného úložiště.

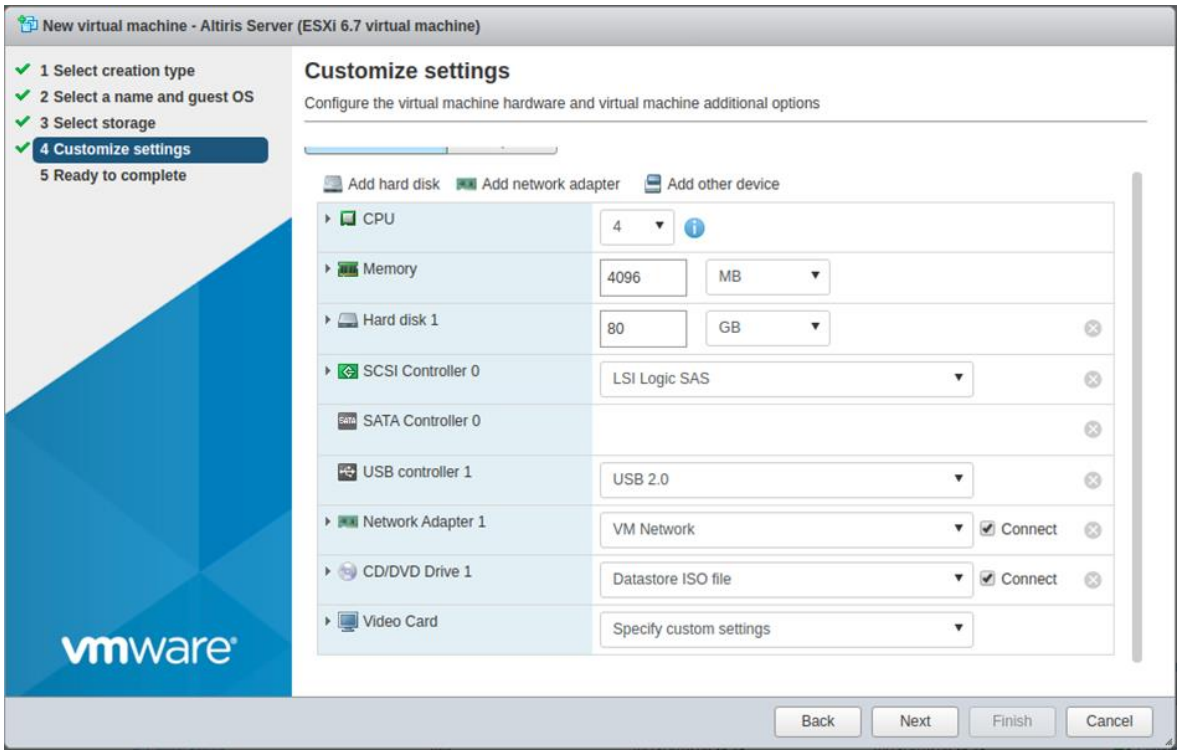
Zde se nachází „Datastore browser“, který umožňuje mimo jiné nahrání souboru do úložiště.



Obrázek 11 – ESXi nahrání ISO souboru zdroj: vlastní

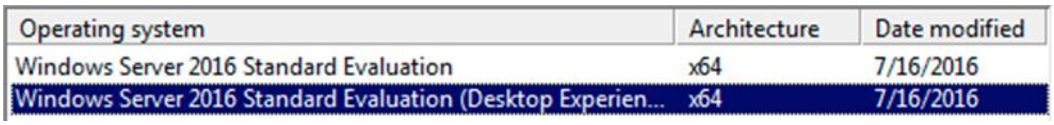
Po nahrání ISO obrazu je třeba vytvořit samotný „virtuální stroj“. To lze realizovat na záložce „Virtual Machines“ pod volbou „Create / Register VM“. Následně je nutno postupně pojmenovat virtuální stroj, vybrat cílový operační systém (v tomto konkrétním příkladě Windows Server 2016) a vybrat úložiště pro daný stroj.

V předposlední, čtvrté části dialogu je třeba přidělit hardwarové prostředky danému virtuálnímu stroji a následně provést klíčový krok, a to vybrat ISO obrazu pro nabootování. Zde to může působit trochu neintuitivně, avšak je třeba u „CD/DVD Drive1“ zakliknout „connect“ a pod nabídkou „Data store ISO file“ vybrat dříve nahraný ISO obraz. Stejně jako je možné vidět na následujícím obrázku.



Obrázek 12 – Konfigurace VM zdroj: vlastní

Poté už stačí pouze zvolit klasicky „Next" a „Finish". Následně se spustí virtuální stroj a provede se klasická instalace Windows serveru (je třeba nezapomenout na stisknutí jakékoliv klávesy pro bootování z CD/DVD media). Instalace je velice podobná ostatním řadám Windows, jako je třeba Windows 10 či Windows 8.1. Toto je méně zajímavá, avšak důležitá část pro nasazení samotného systému pro řízení koncových stanic. A proto, jak již bylo řečeno, zde budou zmíněny pouze zásadnější kroky instalace. V průběhu instalace je třeba vybrat verzi operačního systému.



Obrázek 13 – Verze Windows 2016 zdroj: vlastní

Zde je vhodné vybrat verzi s takzvaným „Desktop Experience", jelikož tato verze obsahuje grafické uživatelské rozhraní (GUI), které napomáhá k pohodlnému spravování Windows serverů.

Jako poslední poznámku k instalaci je vhodné zmínit, že při výběru typu instalace je třeba vybrat volbu „Custom: Install Windows only (advanced)". Což by nebylo až tak podstatné, kdyby po této volbě nenásledovala nabídka, v níž se rozhoduje o tom,

na které úložiště má být systém nainstalován a zde je potřeba správně inicializovat disk. To je pro instalaci zásadní.

Toto je možné v určitých případech učinit přes připravené grafické uživatelské rozhraní, avšak z praxe je známo, že v případě, kdy by disk byl v nějakém neočekávaném stavu či inicializaci, nemusí být chování instalátoru zcela konzistentní. To lze naštěstí vcelku efektivně vyřešit pomocí CLI (Command-line interface), který lze vyvolat klávesovou zkratkou **SHIFT+F10**. Zde je třeba vyvolat následující příkazy.

- ***diskpart*** - Pro spuštění konzolové utility pro práci s disky.
- ***list disk*** - Pro vylistování disků.
- ***select Disk <číslo disku>*** - Pro vybrání disku.
- ***clean*** - Pro smazání celého disku se všemi oddíly.

Po zadání příkazu ***clean*** by mohly následovat příkazy jako ***create partition primary, select partition 1***, ***assign letter=c*** a tak dále. Avšak zde už nic nebrání využít pohodlí grafického uživatelského rozhraní, zavřít příkazový řádek a dokončit instalaci klasicky (je třeba nezapomenout na tlačítko k aktualizaci, které projeví změny v GUI), následně je možné pokračovat vybráním disku, vytvořením oddílu přes tlačítko „new“ a tak dále až do dokončení instalace.

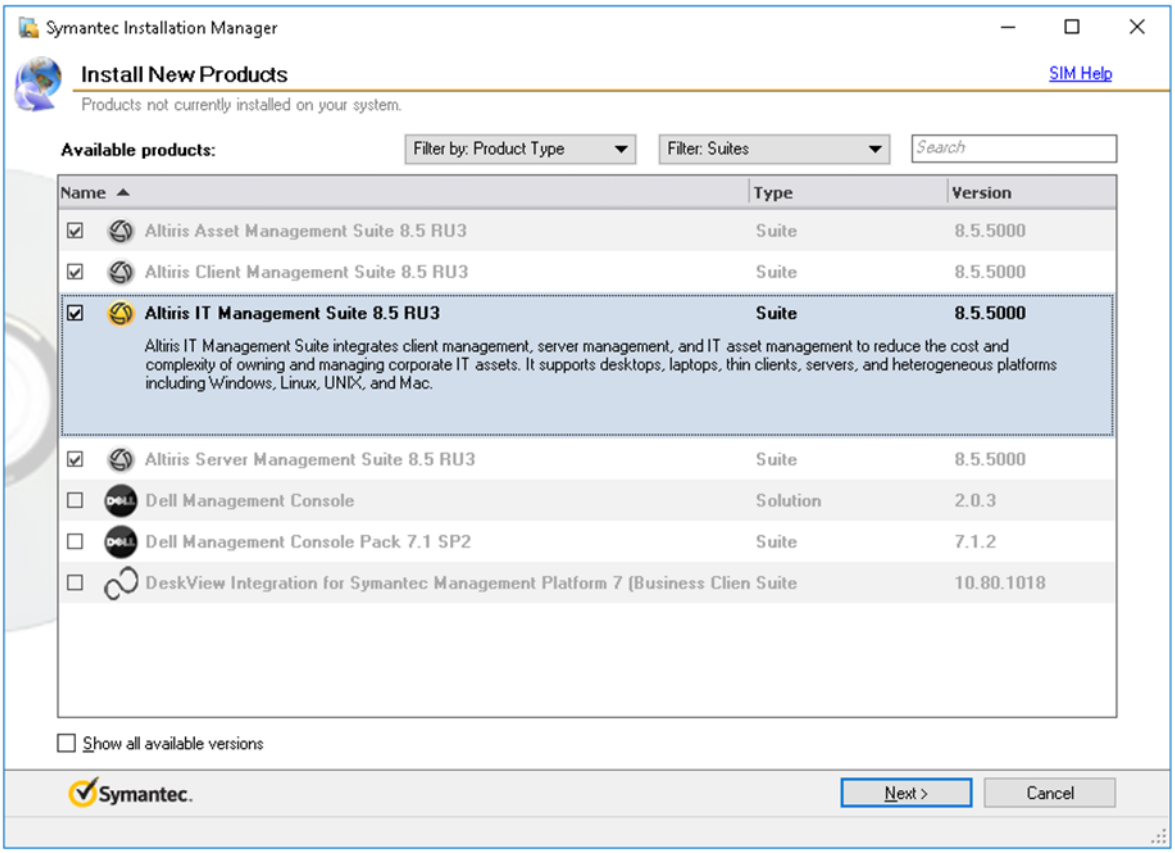
Poté, co je samotný Windows server nainstalován a plně připraven, je možné se vrhnout na přípravu instalace samotného nástroje Symantec Altiris. Což ale znamená, že bude potřeba nainstalovat několik podpůrných prvků před začátkem instalace tohoto nástroje.

3.3. Nasazení softwaru Altiris

Před začátkem instalace je nutné zmínit, že instalační balík včetně doplňků, licencí a dalších podpůrných softwarů byl dodán ze strany korporátního IT oddělení, a proto určité softwarové balíky zde zmíněné mohou podléhat striktním licenčním podmínkám. Tyto balíčky nejsou obsaženy v přiloženém souboru. Přiložený soubor obsahuje nelicencované (trial) verze nebo volně dostupné alternativy.

Pro odstartování procesu nasazení je třeba nejdříve nainstalovat instalačního manažera, což může být trochu zavádějící, avšak instalační manager je velice

užitečným nástrojem, který napomáhá zjednodušit již tak složitý proces instalace. Samotný instalační manažer se instaluje velice snadno jako klasická aplikace za pomocí průvodce. Po spuštění a případné aktualizaci instalačního manažera následuje povědomý instalační dialog, kde je kromě jiného na stránce zvané „Available products“ potřeba zvolit „Altiris IT Management Suite“ včetně „Altiris Server Management Suite“. Zmíněný dialog viz dále.

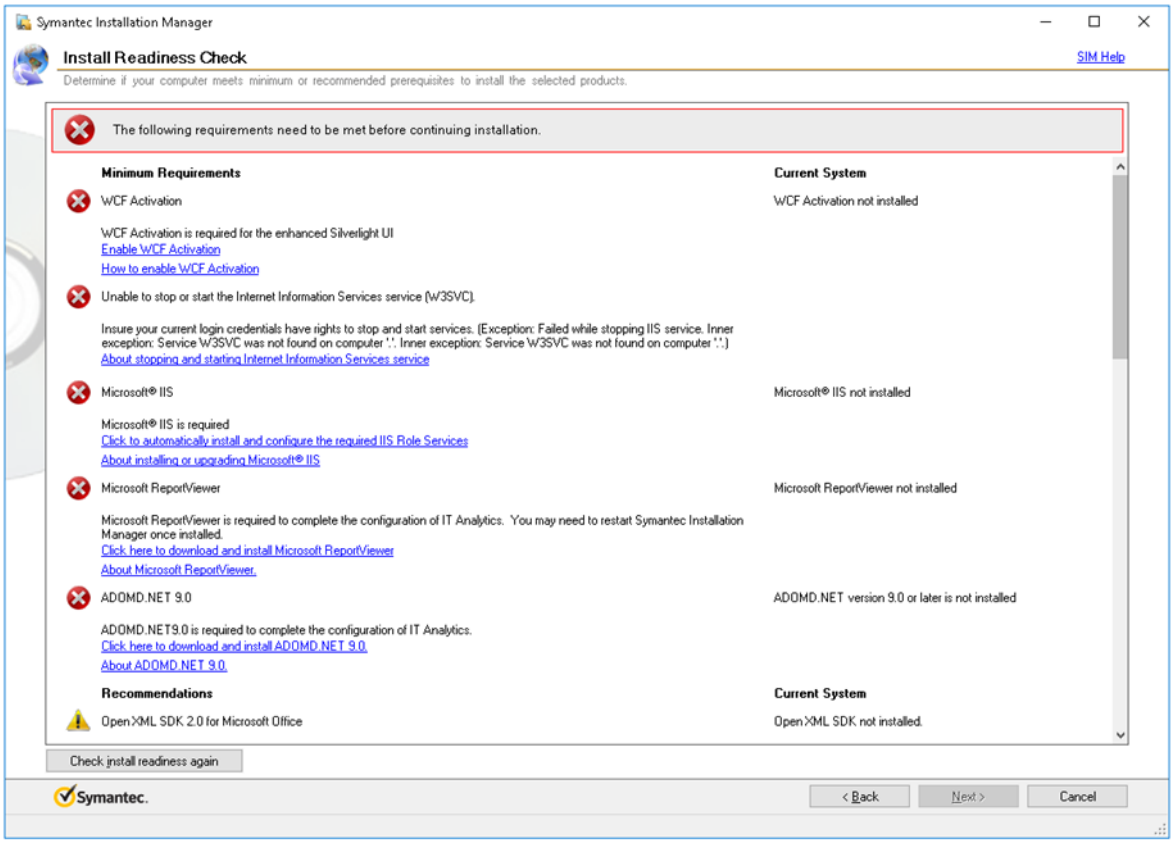


Obrázek 14 – Altiris instalace zdroj: vlastní

V následném sledu dialogů je možné dočíst se konkrétní verzi nasazovaného nástroje (zde 8.5.5) a další podrobné a promo informace jako například: Altiris IT management nástroj slouží pro redukci nákladů a složitosti řízení korporátního IT. Altiris podporuje stolní počítače, notebooky, tenké klienty, servery včetně všech platforem jako je Windows, Linux, Unix a Mac.

Poté už následuje jeden z těžších kroků instalace, a to kontrola všech požadavků pro instalaci softwaru. První kontrola požadavků zpravidla zahlásí několik chyb a doporučení týkající se chybějícího či zastaralého softwaru. Není však třeba se obávat a v uvozovkách pouze doinstalovat potřebný software k pokračování. Zde je z

praxe záhodno podotknout, že známý průběh instalace potřebných softwarových balíčků není zpravidla plynulý a je častokrát provázen různými chybami různého charakteru od chybějících DDL knihoven až po banality, jako jsou z neurčitého důvodu nevyžádaná administrátorská oprávnění a následný pád instalace, což si často vyžádá několikahodinové úsilí a dobrou znalost systému MS Windows. Funkční OVA soubor Windows Server 2016 i s nasazeným softwarem lze nalézt v přílohách práce. Zmíněná Kontrola požadavků nebo také někdy nazývaný jako readiness check vypadá následovně.



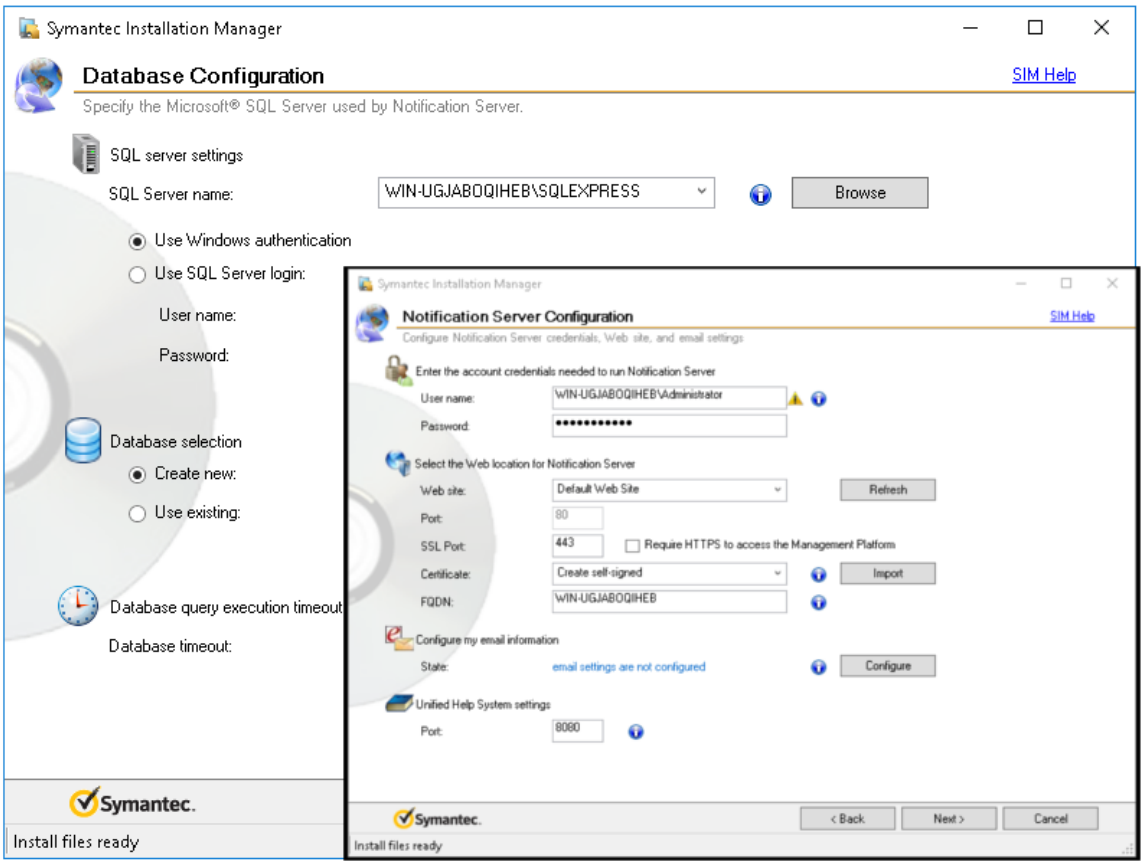
Obrázek 15 – Altiris readiness check zdroj: vlastní

Po úspěšné instalaci všech potřebných balíčků včetně Microsoft SQL (dále MS SQL) databázového serveru a notifikačního serveru s jejich následnou konfigurací lze postoupit dále. Instalace daných serverů zde není ukázaná, jelikož ve firemním prostředí bývá zpravidla již zavedeným standardem. Avšak nutné instalace jsou součástí daného souboru OVA.

Další krok zahrnuje konfiguraci připojení již zmíněného notifikačního serveru, kde je zapotřebí přihlásit se ideálně doménovým, administrátorským účtem pro správnou funkci. Pokud není počítač připojený k doméně, lze místo domény zadat běžně název

počítače. Hned po konfiguraci notifikačního serveru je zapotřebí vyplnit konfiguraci webového serveru. Jedná se v podstatě o server, který bude poskytovat webové rozhraní ke správě celého systému. Altiris nabízí kromě možnosti vytvoření vlastního webového rozhraní či nasazení na separátní server možnost výchozího již nakonfigurovaného webového serveru, což se jeví jako nejpraktičtější varianta. Vytvoření takového serveru lze vcelku snadno prostřednictvím průvodce v instalátoru.

Následně k dokončení instalace zbývá už jen pár kroků a stažení několika gigabytů dat. Nelze však opomenout, že v jednom z posledních kroků je zapotřebí zadat adresu již dříve připraveného SQL serveru. Příklad nastavení může vypadat tak, jak je popsáno níže.

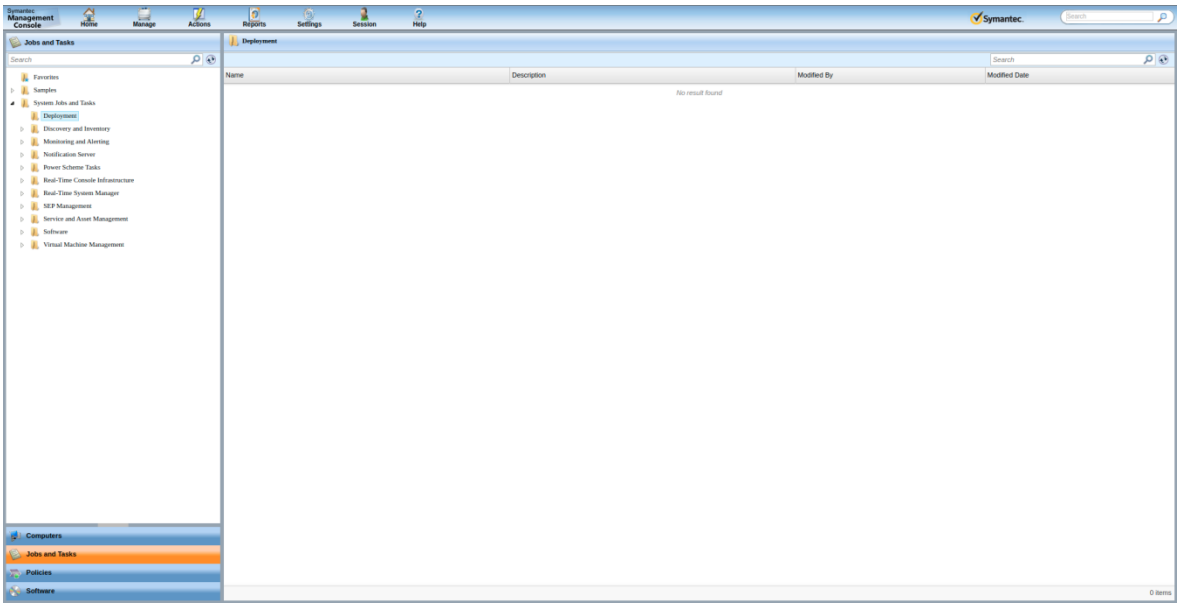


Obrázek 16 – Altiris konfigurace MS SQL zdroj: vlastní

Na obrázku je možné vidět administrátorské přihlašovací údaje k notifikačnímu serveru, dále nastavený výchozí webový server a jeho porty. Proč právě tyto porty a s nimi související protokoly, to již bylo popsáno výše. Je vhodné si povšimnout možnosti volby vynucení zmíněného HTTPS protokolu pro připojení do správy

systému, která probíhá skrze webové rozhraní. Toto nastavení přináší výrazné zlepšení bezpečnosti vnitřní sítě. Jelikož se při správě systému mohou mezi klientem a serverem přenášet nejen data jako MAC adresy, konfigurační soubory a jiná obyčejná data, ale i velmi citlivé údaje, jako jsou hesla, licenční klíče, kontrolní otázky a další, je vhodné využití HTTPS zvážit, poněvadž, jak již bylo zmíněno, HTTP protokol tato data přenáší v nechráněné formě, čímž rapidně usnadňuje potencionální útok. Oproti tomu nakonfigurování HTTPS protokolu s sebou přináší jisté povinnosti v podobě certifikační autority aj. Proto je vhodné důkladně analyzovat veškerá bezpečnostní rizika v dané síti pro následné rozhodnutí, jaký protokol využít pro danou situaci.

K dokončení instalace zbývá již jen pár jednoduchých kroků a po procesu automatického stažení veškerých potřebných komponent je Altiris připraven k používání. Jak již bylo uvedeno, systém je spravován skrze webovou konzoli. Konzoli lze otevřít velice snadno, výchozí webový server tuto konzoli poskytuje na cestě **<IP adresa, případně doména serveru>/Altiris/Console**. Po přihlášení pomocí údajů zadaných při instalaci se naskytne následující pohled.



Obrázek 17 – Altiris overview zdroj: vlastní

Na obrázku lze vidět úvodní stranu Altiris konzole pro správu všech koncových stanic. Popisovat zde celé rozhraní by mohlo být redundantní, proto zde budou zmíněny pouze dvě pravděpodobně nejdůležitější záložky.

Tyto záložky se nachází v levém dolním rohu. Jedná se o záložku „Computers“ a záložku „Jobs and Tasks“. Jak již názvy napovídají, záložka „Computers“ slouží mimo jiné pro vylistování všech počítačů spravovaných Altirisem. Umožňuje ke každému počítači zobrazit veškeré dostupné informace A kromě klasických atributů, jako jsou například MAC a IP adresy, dokáže zobrazit i informace jako posledního přihlášeného uživatele nebo build operačního systému. Následující záložka „Jobs and Tasks“ slouží pro management úloh pro jednotlivé počítače. Příkladem takové úlohy může být instalace jednoduchého softwaru pro několik koncových stanic. Pokud by měl být tento software nainstalován ručně, znamenalo by to v závislosti na počtu koncových stanic úměrné úsilí administrátorů těchto koncových stanic. Oproti tomu, pokud je v Altirisu připraven balíček s instalací daného softwaru, znamená to pro správce pouze pár kliknutí k přidělení dané úlohy či balíčku na jednotlivé koncové stanice, přičemž po přidělení bude instalace provedena zcela automaticky. Jak již je možné tušit, základem pro automatickou instalaci softwaru či nasazení operačního systému je vytvoření instalačního balíčku.

3.4. Vytvoření instalačního balíčku

Vytvoření instalačního balíčku zahrnuje již zmíněné předdefinování jednotného softwaru, který může být následně hromadně a zcela automaticky instalován na koncová zařízení. Bez těchto balíčků by byl nástroj Altiris praktický bezvýznamný. Nejzajímavějším softwarem pro instalaci je nepochybně operační systém. Proto zde bude popsána jedna z metod vytvoření hardwarově nezávislého instalačního balíčku včetně prostředí WinPE pro instalaci Windows 10. Jelikož Windows 10 je nejrozšířenějším operačním systémem, byl zvolen jako zástupce pro ukázku deploymentu.

Vytvoření instalačního balíčku je jednou z nejobtížnějších věcí při automatickém deploymentu. Pro úspěšné automatické nasazení operačního systému je zapotřebí udělat několik desítek kroků a úspěšně projít celým procesem vytvoření instalačního balíčku. Typicky na takovéto úloze pracuje tým koordinovaných IT administrátorů. Zde budou popsány pouze hlavní kroky a jejich úskalí tak, aby bylo možné celý proces zopakovat.

3.4.1. Skriptová instalace

Prvním krokem je příprava ISO souboru (také ISO nebo ISO obraz) skriptové instalace Windows 10. K přípravě instalace Windows 10 pomocí skriptu bude potřeba hned několika nástrojů. Pomocí těchto nástrojů bude nejdříve vytvořen klasicky ISO soubor. Daný ISO soubor bude následně použit pro vytvoření souboru automatické instalace Windows, který se již importuje do systému Altiris.

Jak již bylo zmíněno, první krok spočívá v přípravě samotného ISO souboru, který má být dále distribuován. ISO soubor Windows 10 lze vytvořit několika způsoby. Jednak jednoduše stáhnout na stránkách firmy Microsoft [59], vytvořit pomocí nástroje zvaného „media creation tool“ taktéž od společnosti Microsoft, případně lze klasicky vytvořit ISO soubor zachycením z již modifikovaného systému pomocí programu sysprep.exe. Tímto způsobem lze dosáhnout toho, aby daný systém byl již modifikován, odpovídal standardům dané společnosti a výsledný soubor zůstal stále hardwarově nezávislý.

Druhý krok spočívá v modifikaci daného ISO souboru, tak aby byl autoinstalační. To lze udělat tak, že se do daného obrazu přidá XML soubor s názvem Autounattend (někdy nazýván i „answer file“). [59] Modifikace ISO obrazu není úplně triviální operací. Většina softwaru pro práci s ISO soubory nabízí modifikaci pouze do velikosti 300 MB, avšak v praxi se na toto osvědčil jeden z mála nástrojů zvaný Anyburn [60], který v bezplatné verzi modifikuje ISO soubory jakékoliv velikosti.

Samozřejmě před přidáním daného Autounattend souboru je třeba tento soubor vytvořit. To lze učinit několika způsoby. Jelikož se jedná o klasický XML soubor, lze ho jednoduše napsat v textovém editoru, avšak tvorba obsáhlého XML souboru běžným způsobem v textovém editoru není zcela adekvátní, a proto existuje několik softwarových nástrojů pro jeho snadné vytvoření. Jedna možnost je pomocí dále zmíněného nástroje, z daného ISO obrazu konvertovat soubor s koncovkou .WIM (Windows Imaging Format). To umožní následnou lehčí implementaci XML souboru přímo pro danou verzi Windows v nástroji „Windows System Image Manager“.

Nejdříve je třeba tento nástroj získat. To lze vcelku snadno stažením balíčku s názvem Windows ADK (Windows Assessment and Deployment Kit), který obsahuje i další

potřebné nástroje. Stažení lze opět provést přímo ze stránek firmy Microsoft, [59] pro verzi Windows 10 je zapotřebí ideálně verze 8.5 RU3. Instalace daného softwaru je zcela typická pro Windows prostředí. Kromě nutnosti akceptování licenčních ujednání je třeba při výběru instalovaných nástrojů zaškrtnout volby „Deployment Tools“ a „Windows Preinstallation Environment” pro další použití.

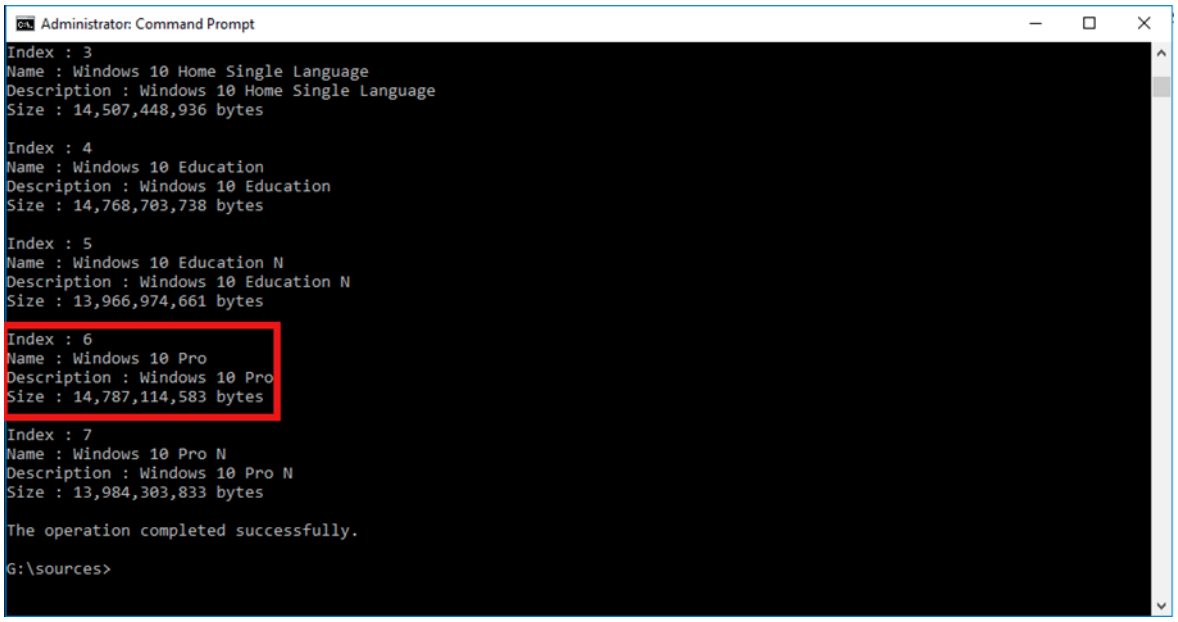
Následně je třeba vytvořit daný .WIM soubor. Prvním krokem k vytvoření tohoto souboru je extrahování daného ISO obrazu například pomocí programu WinRar. [61] Poté je třeba vyhledat soubor s názvem „install.esd“, který se nachází v adresáři „sources“. Je možné si povšimnout, že daný soubor „install.esd“ je největším souborem z celého obrazu, poněvadž samotné MS Windows jsou umístěny v podstatě v tomto souboru. Pro zajímavost se lze znovu pomocí programu WinRar do tohoto souboru podívat, přičemž je vidět, že tento soubor obsahuje jednotlivé verze daného systému. Dále musí být použit CLI, kde je třeba dojít až na rozbalený ISO soubor do dané složky „Sources”. Zde se nachází daný soubor „install.esd“.

Pro konverzi je nejdříve nutno zjistit index dané verze Windows (v konkrétním případě bude instalována verze Windows 10 Pro, jak je to ve firemním prostředí zvykem). Ke zjištění daného indexu slouží následující příkaz programu DISM.

dism /Get-WimInfo /WimFile:install.esd

Pro úspěšné provedení příkazu je nutné nacházet se v daném adresáři „Sources”.

Výstup je následující.

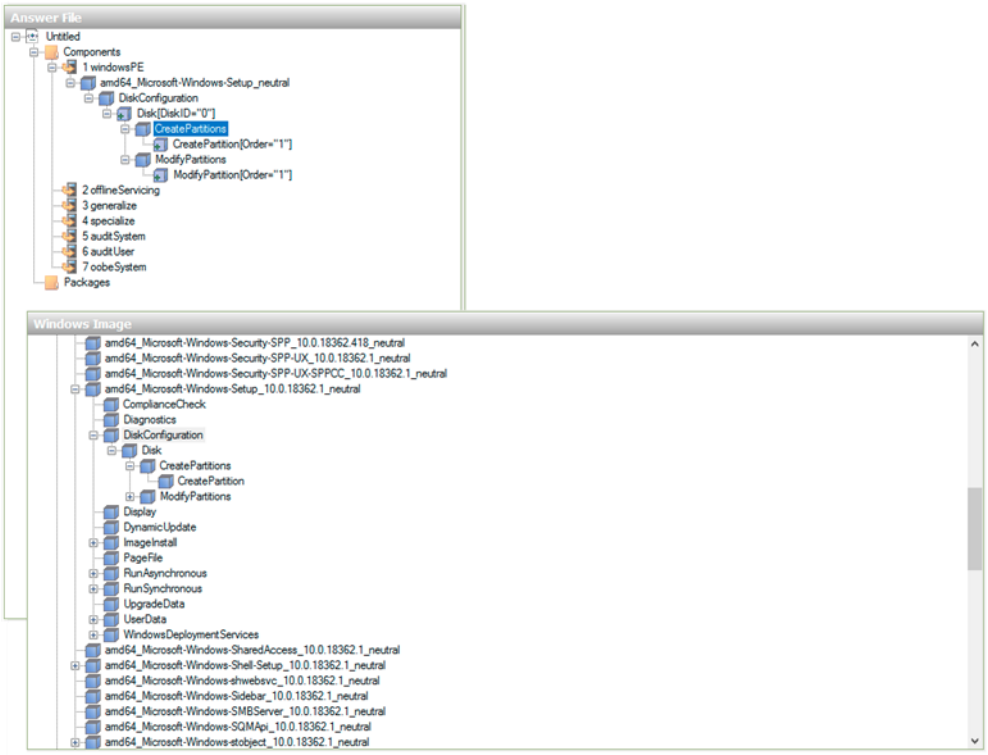


Obrázek 18 – Index dané verze zdroj: vlastní

V tomto konkrétním případě byl index 6 pro verzi Pro. To je nutné znát pro finální operaci, která vytváří daný soubor .WIM a zahájena bude jednoduchým příkazem. Pro řešený případ daný příkaz vypadá následovně.

dism /export-image /SourceImageFile:install.esd /SourceIndex:6 /DestinationImageFile:install.wim /Compress:max /CheckIntegrity

Po provedení daného příkazu je soubor s názvem „install.wim" hotov. Lze ho tedy jednoduše otevřít v již zmíněném nástroji „Windows System Image Manager", který je součástí balíku Windows ADK. V daném předem připravenému souboru lze jednoduše automatizovat a přednastavovat jednotlivé kroky jako například práce s disky, vytvoření jednotlivých oddílů disku, přidělení písmena disku a další. Daný nástroj má několik panelů, avšak uvedeny budou dva nejdůležitější.



Obrázek 19 – Windows Systém Image Manager zdroj: vlastní

Panel s názvem „Answer file“ slouží mimo jiné pro tvorbu daného XML souboru, oproti tomu panel s názvem „Windows Image“ tvoří seznam všech možných automatizovaných operací. Zde je vhodné uvést, že soubor „install.wim“ nyní poslouží pouze jako pomocný soubor pro vytvoření daného XML souboru, i když jeho možnosti využití jsou mnohem širší.

Výstupem daného nástroje je XML soubor. Ukázkový Autounattend soubor lze nalézt například na autorově Githubu. [62] Daný Autounattend mimo jiné automaticky nakonfiguruje Windows 10 s jedním oddílem disku o velikosti 40 GB označeným jako primární a přiděleným písmenem C. Dále projde veškerá inicializační nastavení a vytvoří uživatele s názvem Administrátor a heslem „password”. Dále na tohoto uživatele nastaví funkci zvanou Autologon. Daný XML soubor stačí pouze přidat do cílového ISO souboru nebo vytvořeného USB bootovacího zařízení, čímž vzniká autoinstalační ISO obraz.

Tato funkce je pro IT administrátory v každodenním životě opravdu klíčová, jelikož automatizuje proces a výrazně zkracuje dobu od zavedení bootovacího média po plnou připravenost systému. Co je vhodné zmínit před dalším krokem, je to, že v daném XML souboru ani v žádné jiné operaci nebude zobrazeno připojení počítače

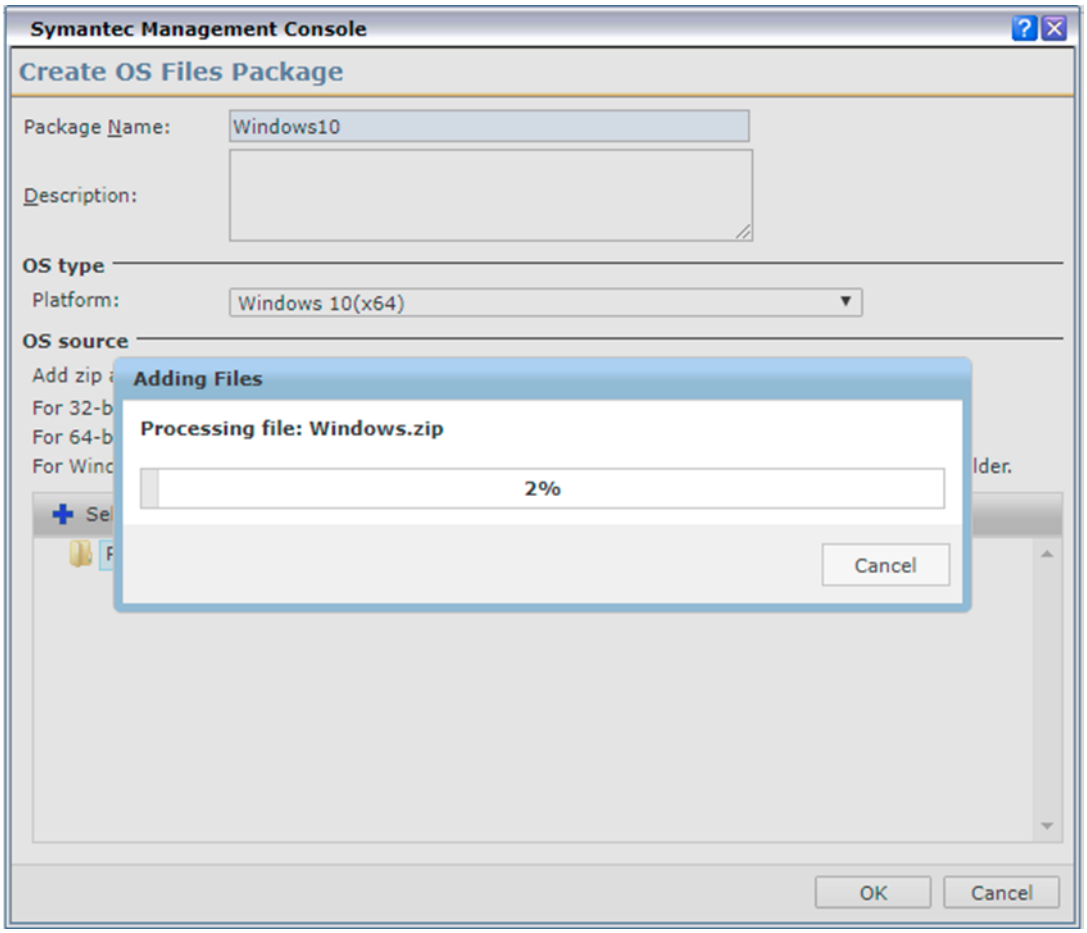
k podnikové doméně active directory, přestože je to běžnou praxí. Toto nebude zobrazeno hned z několika důvodů. Jednak v podnikové sféře by to mohlo znamenat bezpečnostní riziko a v domácím prostředí takovéto připojení není možné, ba je dokonce bezvýznamné. Navíc se zpravidla jedná pouze o triviální přidání atributu a vyplnění údajů doménového administrátora.

Poté, co je připraven instalační obraz systému Windows 10, lze ho importovat do systému Altiris a vytvořit prostředí pro zavedení daného obrazu.

3.4.2. Altiris instalační balíček

Úloha automatického zavedení operačního systému pomoci PXE a další konfigurace je rozsáhlý proces, kterému se v korporátních společnostech věnují celé týmy lidí. Zde budou popsány převážně postupy z autorova úhlu pohledu jako IT plant administrátora tak, jak probíhaly při implementaci daného systému v ZF Frýdlant. Je třeba mít na paměti, že pro funkčnost daného systému je nutné, aby spolupracovalo hned několik týmů současně. Jedná se hlavně o vývojový tým, Connectivity tým a IT plant tým. Je třeba správně nakonfigurovat hned několik nástrojů, jsou jimi zejména TFTP a DHCP servery, tak aby celý systém fungoval stabilně a bezpečně.

Prvním krokem celého procesu vytvoření balíčku pro automatický deployment Windows 10 je import daného ISO obrazu do systému Altiris. To lze udělat v sekci Settings>OS Files>Add Files, viz obrázek 20.

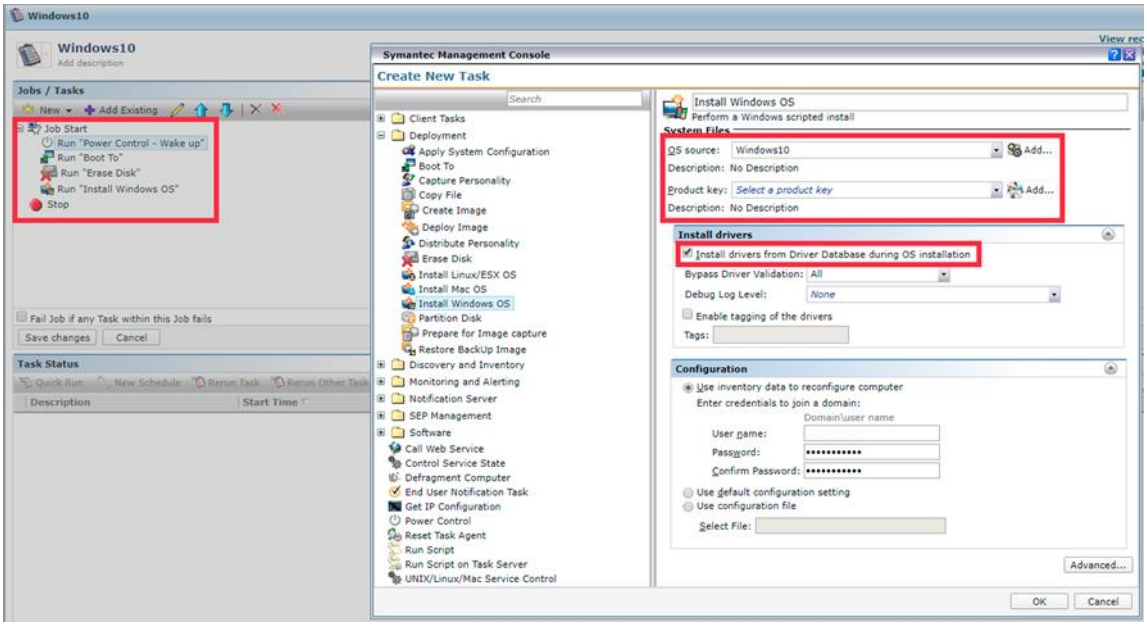


Obrázek 20 – Upload ISO obrazu zdroj: vlastní

Zde je několik možností importu, přitom nejvhodnějšími dvěma možnostmi jsou nahrání přímo ISO obrazu, jelikož server, na kterém Altiris běží, je zpravidla umístěn v síti, je také možnost nahrání zip archivu s následným rozbalením na straně daného serveru. Lze vidět, že v dialogu je třeba upřesnit verzi operačního systému a několik dalších podrobností.

Po úspěšném importu následuje příprava Preboot prostředí. To lze v systému Altiris udělat pro Windows operační systémy připraveným průvodcem na cestě Settings>Deployment>Preboot Configuration. V rámci průvodce je nutné stažení několik dalších nástrojů pro úspěšné nastavení. V tomto kroku je pro správnou funkci zavedení operačního systému ze sítě zásadní konfigurace dalších převážně síťových záležitostí, zejména pak DHCP serveru. Po úspěšném ukončení poskytne průvodce kromě jiné cestu TFTP serveru pro zavedení daného systému, která je zpravidla vyžadována pro DHCP server (viz. kapitola 2.5). Před konečným vytvořením celé úlohy je ještě vhodné přidat v sekci „OS Licenses“ licenční klíče pro daný systém. Pak již stačí zahájit tvorbu dané úlohy.

To lze velice jednoduše takzvaně „naklikat“ v sekci Manage>Jobs And Tasks, kde je vhodné vytvořit novou složku ve složce nový „klient task” a zde už je možné konfigurovat celý balíček po jednotlivých úlohách. Konfigurace vypadá následovně.



Obrázek 21 – Tvorba instalačního balíčku zdroj: vlastní

Jak lze vidět na obrázku, vytvořit velice jednoduchý balíček či proces celé instalace je možné ve čtyřech krocích. Zapnutí počítače, restartování s následným startem PXE, kompletní smazání všech disků v počítači a spuštění připravené skriptové instalace Windows 10.

Na obrázku je zaznamenána konfigurace kroku pro instalaci Windows 10, zde je nutné zvolit již dříve předpřipravené soubory s operačním systémem a licenčním klíčem. Jako jeden z posledních kroků je třeba zaškrtnout možnost instalace ovladačů z předpřipravené databáze. Pro velkou část typických korporátních zařízení jsou veškeré ovladače již součástí dané databáze. Pokud tomu tak není, lze ovladače jednoduše do dané databáze přidávat. Popřípadě Windows 10 na převážné většině nových zařízení nainstaluje veškeré ovladače v rámci svých aktualizací, pokud politika firmy nestanoví jinak.

Výše uvedený postup instalace bude fungovat pouze za předpokladu již registrované koncové stanice. Registraci stanice je možné provést několika způsoby, například předdefinovaním (zadání jména a MAC adresy stanice) či instalací klienta, kterého lze vytvořit v instalačním manageru. Avšak zpravila je žádoucí, aby bylo možné instalovat

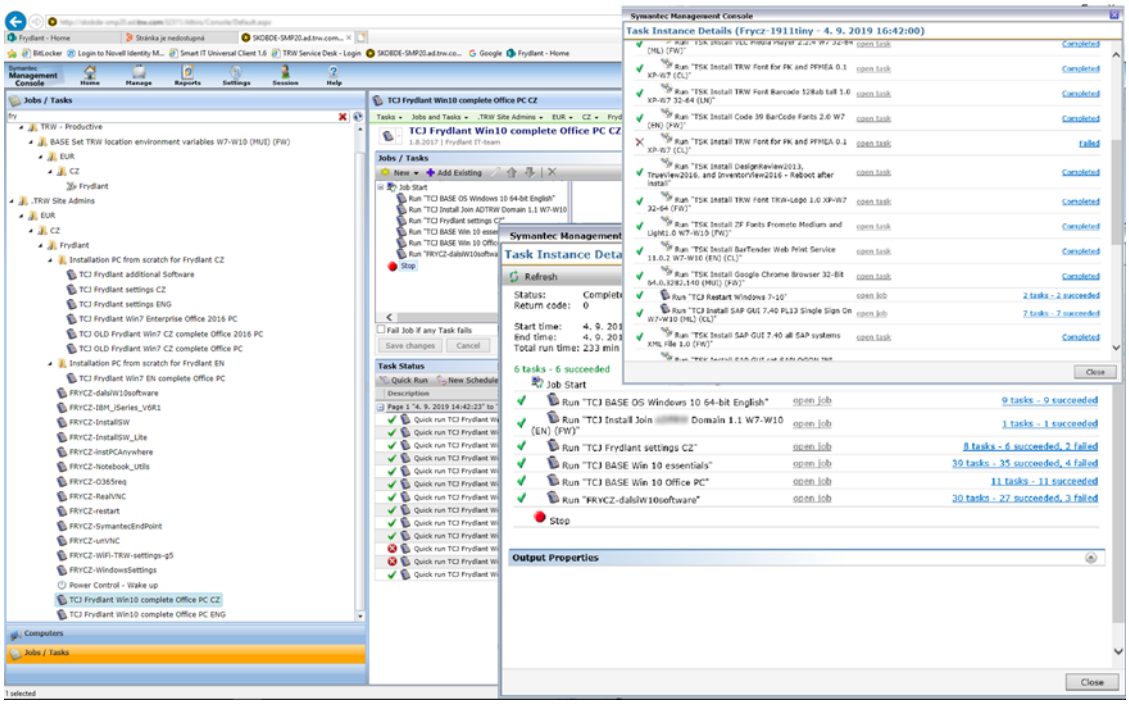
zcela neznámé stanice v síti (tím je zároveň i registrovat). Jsou zde možnosti v sekci „Initial Deployment", přiřadit jednotlivou úlohu pro neznámé stanice. Pak už stačí jen takzvaně „nabootovat" z PXE.

3.5. Ostatní software

Po úspěšné instalaci operačního systému vzniká potřeba instalace další softwarových produktů, jako jsou například klienti pro podnikové informační systémy (například SAP nebo BPCS AS/400), kancelářské balíky, mediální přehrávače, CAD nástroje v mnoha odvětvích jako strojírenství, stavebnictví a mnoho dalších.

Samotné instalační balíčky jednotlivých softwarů lze nejčastěji již vytvořené importovat nebo velice jednoduše vytvářet z klasických .exe, .msi a dalších souborů. Příklad lze nalézt na stránkách knowledge.broadcom.com. [63]

Na záložce Jobs and Tasks z obrázku 16 – Altiris overview lze zaznamenat, že samotné instalační balíčky je možné jednoduše seskupovat do složek a tvořit tak stromovou strukturu jako například u file systémů. Do každého balíčku lze přidat několik úloh či podmínek tak, aby tvořily logický celek. Jednotlivé balíčky můžou být do sebe vnořeny a vytvářeny tak složité struktury instalačních procesů. Pro lepší představu slouží následující obrázek.



Obrázek 22 – Altiris ZF Frýdlant

Na obrázku lze vidět již dokončený proces deploymentu operačního systému společně se všemi dalšími softwarovými balíčky v ZF Frýdlant. Kromě klasického softwaru instalace obsahuje i připojení k firemní doméně, zavedení několika certifikátů a autentifikačních tokenů pro ověření v korporátní síti. Je možné si také všimnout, že určité úlohy skončily chybou. U některých je to chování žádoucí, například software pro notebooky nemůže být nainstalován na stolním počítači, u jiných toto představuje problém a je třeba úlohu, která selhala, provést ručně či hledat její příčinu. Je záhodno poznamenat, že velký počet reportovaných selhání, který je vidět na obrázku, tvoří podmínky, které ve chvíli, kdy se podmínka vyhodnotí jako „false", je daná úloha (vyhodnocení podmínky) označena jako „failed", přestože je toto chování žádoucí.

5. Shrnutí výsledků

Hlavní cíle práce byly splněny. Systém pro správu koncových zařízení se ve společnosti ZF Frýdlant povedlo úspěšně implementovat. Proces celé implementace od odsouhlasení rozpočtu až po uzavření projektu a prohlášení systému za stabilní trval zhruba šest měsíců. Během celého procesu probíhal chod IT oddělení zcela stejně jako za běžného provozu. V průběhu implementace nebyla omezena žádná jiná služba celého IT oddělení až na pár krátkodobých výpadku v případě restartu síťových služeb, a to pouze v situacích, kdy to bylo opravdu nezbytné. Virtualizační platforma VMware ESXi byla taktéž úspěšně implementována nejen pro systém endpoint managementu, ale i pro další technologie nezbytné pro chod celého závodu.

Proces implementace provázelo několik úskalí, zejména v případě kompatibility hardwaru pro VMware ESXi, dále pak několik nejasných obtíží ve chvíli instalace systému Altiris a konfigurace DHCP. Avšak veškeré tyto problémy se podařilo překonat a oba systémy úspěšně nasadit. VMware ESXi se dle očekávání ukázal jako velice praktický nástroj pro serverovou virtualizaci a potvrdil tak své právoplatné místo mezi elitou v oboru. Na druhou stranu je mu třeba vytknout menší škálu podporovaného hardwaru, která může zvyšovat náklady na daný systém.

Altiris, systém pro správu koncových stanic, se ujal velice dobře. Automatický deployment operačního systému velice usnadňuje chod IT oddělení. Dnes je automatický deployment operačního systému již standardem a využívá se v běžném provozu IT oddělení. Je třeba zmínit, že se Altiris zejména v začátcích ukázal jako systém velice náchylný na síťové a jiné chyby. Avšak při správné konfiguraci sítě systém funguje dobře a velice stabilně. Nasazení nejen Altirisu, ale všeobecně nástroje pro správu koncových zařízení se ukázalo jako velice dobrý krok pro budoucí rozvoj IT infrastruktury v ZF Frýdlant.

6. Závěry a doporučení

Je dobré mít na paměti, že v podnikové sféře je třeba dbát nejen o koncová zařízení, ale také o data a informace v nich uchovávané. A to jak o samotná data či informace, tak zejména o jejich bezpečnost. V poslední době s novými nařízeními, jako je například GDPR, je třeba starat se mimo jiné o obsah daných dat v zařízení. Tomuto se rychle přizpůsobují i nástroje pro správu těchto zařízení. Do budoucna lze očekávat stálou expanzi nástrojů pro endpoint management a další integraci s nástroji pro data management. Lze očekávat stále rostoucí trend v automatizaci správy těchto zařízení a přesun jednotlivých kroků pro udržení daných zařízení v chodu z koncového uživatele na určitého supervizora. Tedy na článek, který bude automatizován a pouze za dohledu IT správců bude řídit, aplikovat a dohlížet na pravidla stanovená společností.

Lze také předpokládat stabilní vývoj a stále rostoucí investice ve firemním prostředí do virtualizačních nástrojů a technologií k nim potřebných. Zejména pak investice do serverové virtualizace a záležitostí s ní spojených.

Altiris jako nástroj pro endpoint management je možné doporučit pro nasazení v podnikové sféře, přestože se jedná o starší nástroj. Altiris se osvědčil jako mocný a přitom stále jednoduchý a elegantní nástroj pro deployment operačního systému a dalších softwarových balíků.

VMware ESXi virtualizační nástroj, jako hypervisor typu jedna, je profesionální nástroj na vysoké úrovni a bez větších problémů ho lze doporučit do průmyslového prostředí s vyššími nároky jak na výkon, tak na správu systému. Ovšem je třeba míti na paměti i veškerá úskalí samotné virtualizace i daného nástroje.

Nakonec by bylo vhodné zmínit, že tato práce se stala velkým osobním přínosem a výrazně přispěla k mému osobnímu rozvoji i dalšímu profesnímu směřování. Nejen tato práce, ale i celé mé několikaleté působení v ZF Frýdlant bylo velkým přínosem a zároveň inspirací pro vytvoří této práce. Hlavní inspirací pro vytvoření této práce byla potřeba automatizovat dané procesy a odlehčit tak IT správcům v dané společnosti. Jsem tedy rád, že se tento cíl podařilo realizovat, a tím v ZF Frýdlant zcela

automatizovat důležité procesy, které probíhají každý den nejen v IT sféře ZF Frýdlant, ale i ve spoustě jiných centrech po celém světě.

7. Seznam použité literatury

[1] K. Hess, *Unified Endpoint Management For Dummies® IBM Limited Edition*, 1. vyd. John Wiley & Sons, Inc., 2017.

[2] S. Rob, D. Rich, S. Chris, a B. Manjunath, „Magic Quadrant for Unified Endpoint Management Tools", *Gartner*, srp. 06, 2019. https://www.gartner.com/en/documents/3956003/magic-quadrant-for-unified-endpoint-management-tools (viděno dub. 26, 2020).

[3] L. Joyce, „Unified Endpoint Management (UEM) : A Beginner's Guide | SYNDES", *Syndes Technologies*, srp. 15, 2019. https://syndes.biz/blog/knowledge-base/unified-endpoint-management-uem-a-beginners-guide/ (viděno dub. 26, 2020).

[4] „What is an Endpoint?", *paloaltonetworks*. https://www.paloaltonetworks.com/cyberpedia/what-is-an-endpoint (viděno dub. 26, 2020).

[5] „What is Unified Endpoint Management (UEM)? | UEM solutions - ManageEngine Desktop Central". https://www.manageengine.com/products/desktop-central/unified-endpoint-management-solutions.html (viděno dub. 26, 2020).

[6] A. Joseph, „Device Management", *archive.today*, srp. 01, 2012. http://archive.is/n6sk (viděno dub. 26, 2020).

[7] B. Ben, „Whitelisting, Blacklisting and Your Security Strategy", *Twistlock*, led. 02, 2019. https://www.twistlock.com/2019/01/02/whitelisting-blacklisting-security-strategy/ (viděno dub. 26, 2020).

[8] B. Shebaro, O. Oluwatimi, a E. Bertino, „Context-Based Access Control Systems for Mobile Devices", *IEEE Trans. Dependable and Secure Comput.*, roč. 12, č. 2, s. 150–163, bře. 2015, doi: 10.1109/TDSC.2014.2320731.

[9] R. Afreen, „Bring Your Own Device (BYOD) in Higher Education: Opportunities and Challenges", *Course Coordinator (MCA), Millennium Institute of Management*, roč. 3, č. 1, s. 5, bře. 2014.

[10] N. Jiří, „BYOD: Poraďte si s vlastními přístroji zaměstnanců", *ICT manažer*, led. 02, 2012. http://www.ictmanazer.cz/2012/01/byod-poradte-si-s-vlastnimi-pristroji-zamestnancu/ (viděno dub. 26, 2020).

[11] K. W. Miller, J. Voas, a G. F. Hurlburt, „BYOD: Security and Privacy Considerations", *IT Prof.*, roč. 14, č. 5, s. 53–55, zář. 2012, doi: 10.1109/MITP.2012.93.

[12] Symantec, „From 10-K Annual Report". Symantec Corp, Viděno: dub. 26, 2020. [Online]. Dostupné z: https://help.symantec.com/cs/itms8.5/SMPLAT/v45852441_v125258922/How-IT-Management-Suite-works?locale=EN_US.

[13] „About IT Management Suite", *https://help.symantec.com/*. https://help.symantec.com/cs/itms8.5/SMPLAT/v45852432_v125258922/About-IT-Management-Suite?locale=EN_US (viděno dub. 26, 2020).

[14] „Altiris™ Deployment Solution from Symantec". úno. 2018, [Online]. Dostupné z: http://www.redicsa.com/pdf/Symantec/Endpoint-Management-Altiris/Client-Management/Deployment-Solution.pdf.

[15] J. A. Gil-Martinez-Abarca, F. Macia-Perez, D. Marcos-Jorquera, a V. Gilart-Iglesias, „Wake on LAN over Internet as Web Service", in *2006 IEEE Conference on Emerging Technologies and Factory Automation*, Prague, Czech Republic, zář. 2006, s. 1261–1268, doi: 10.1109/ETFA.2006.355397.

[16] „History of Altiris, Inc. – FundingUniverse". http://www.fundinguniverse.com/company-histories/altiris-inc-history/ (viděno dub. 27, 2020).

[17] „Symantec Corp". Symantec corp, kvě. 21, 2008, [Online]. Dostupné z: http://d1lge852tjjqow.cloudfront.net/NasdaqGlobal-SYMC/ec83c678-2f06-40b4-afaf-a0222a4addf4.pdf.

[18] *Preboot Execution Environment (PXE) Specification*, 2.1. Intel Corporation, 1999.

[19] Ken, „PXE Boot, What is PXE? How does it work?", *Linuxhit.com*, pro. 05, 2019. https://linuxhit.com/pxe-boot-what-is-pxe-how-does-it-work/ (viděno dub. 28, 2020).

[20] L. Avramov a P. Maurizio, *The policy driven data center with ACI: architecture, concepts, and methodology*. Indianapolis, IN: Cisco Press, 2015.

[21] L. John, „MS denies secure boot will exclude Linux", zář. 23, 2011. https://www.theregister.co.uk/2011/09/23/ms_denies_uefi_lock_in/ (viděno dub. 27, 2020).

[22] V. Zimmer, M. Rothman, a S. Marisetty, *Beyond BIOS: developing with the Unified Extensible Firmware Interface*, 2nd ed. Hillsboro, Or: Intel Press, 2010.

[23] D. McElheran, „UEFI, BIOS, GPT, MBR - What's the Difference?", *Fossbytes*, pro. 31, 2016. https://fossbytes.com/uefi-bios-gpt-mbr-whats-difference/ (viděno dub. 27, 2020).

[24] C. Per, „Protocol Definition", *TechTerms*, bře. 29, 2019. https://techterms.com/definition/protocol (viděno dub. 27, 2020).

[25] P. J. Leach, T. Berners-Lee, J. C. Mogul, L. Masinter, R. T. Fielding, a J. Gettys, „Hypertext Transfer Protocol -- HTTP/1.1". https://tools.ietf.org/html/rfc2616 (viděno dub. 27, 2020).

[26] H.-C. Chua, „In Introduction to HTTP Basics", říj. 20, 2009. https://www.ntu.edu.sg/home/ehchua/programming/webprogramming/HTTP_Basics.html (viděno dub. 27, 2020).

[27] E. Asgout, „Active attacks", dub. 10, 1996. http://www.pvv.org/~asgaut/crypto/thesis/node11.html (viděno dub. 27, 2020).

[28] „Zabezpečení webu protokolem HTTPS - Nápověda Search Console". https://support.google.com/webmasters/answer/6073543?hl=cs (viděno dub. 27, 2020).

[29] „What is Transport Layer Security (TLS)?", *Cloudflare*. https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/ (viděno dub. 27, 2020).

[30] „Chapter 12 Securing Instant Messaging Using TLS and Legacy SSL (Sun Java System Instant Messaging 7.2 Administration Guide)". https://docs.oracle.com/cd/E19566-01/819-4412/achbu/index.html (viděno dub. 27, 2020).

[31] „Networking for WordPress Administrators - WordPress Security", *Wordfence*, led. 25, 2016. https://www.wordfence.com/learn/networking-for-wordpress-administrators/ (viděno dub. 27, 2020).

[32] C. D. Graziano, „A performance analysis of Xen and KVM hypervisors for hosting the Xen Worlds Project", Master of Science, Iowa State University, Digital Repository, Ames, 2011.

[33] E. Mike, A. Matthew, F. Carlos Felipe Frana da, G. Marc, P. Veerendra, a S. Michael, *Smarter Data Centers: Achieving Greater Efficiency*. Smarter Data Centers: Achieving Greater Efficiency, 211n. l.

[34] Admin, „The Different Types of Virtualization in Cloud Computing – Explained", *redswitches.com*, bře. 26, 2020. https://www.redswitches.com/blog/different-types-virtualization-cloud-computing-explained/ (viděno dub. 27, 2020).

[35] B. Golden, *Virtualization For Dummies, 3rd HP Special Edition*, roč. 3 část. Wiley Publishing, Inc, 2011.

[36] R. Y. Ameen a A. Y. Hamo, „Survey of Server Virtualization", č. 3, s. 10, 2013.

[37] J. Sahoo, S. Mohapatra, a R. Lath, „Virtualization: A Survey on Concepts, Taxonomy and Associated Security Issues", in *2010 Second International Conference on Computer and Network Technology*, Bangkok, Thailand, 2010, s. 222–226, doi: 10.1109/ICCNT.2010.49.

[38] B. Steve, „Virtualization for Newbies: Five Types of Virtualization", říj. 03, 2013. http://www.globalknowledge.com/us-en/resources/resource-library/articles/virtualization-for-newbies-five-types-of-virtualization/ (viděno dub. 27, 2020).

[39] Kelser, „The 7 Types of Virtualization", *Kelser*, lis. 18, 2015. https://www.kelsercorp.com/blog/the-7-types-of-virtualization (viděno dub. 27, 2020).

[40] „What is a hypervisor?", *redhat.com*. https://www.redhat.com/en/topics/virtualization/what-is-a-hypervisor (viděno dub. 27, 2020).

[41] VapourApps, „What is Hypervisor and what types of hypervisors are there?", *Vapour-Apps.com*, kvě. 13, 2016. https://vapour-apps.com/what-is-hypervisor/ (viděno dub. 27, 2020).

[42] W. Graniszewski a A. Arciszewski, „Performance analysis of selected hypervisors (Virtual Machine Monitors - VMMs)", *International Journal of Electronics and Telecommunications*, roč. 62, č. 3, s. 231–236, zář. 2016, doi: 10.1515/eletel-2016-0031.

[43] Bipin, „Difference between vSphere, ESXi and vCenter", *MustBeGeek*, srp. 24, 2012. https://www.mustbegeek.com/difference-between-vsphere-esxi-and-vcenter/ (viděno dub. 27, 2020).

[44] V.-C. Steven J., „Hypervizory přímo na holém hardwaru: Který je pro vás nejvhodnější?", *Computerworld.cz*, led. 28, 2017. https://computerworld.cz/software/hypervizory-primo-na-holem-hardwaru-ktery-je-pro-vas-nejvhodnejsi-53602 (viděno dub. 27, 2020).

[45] „VMware ESX Server". VMware, Inc., 2007 1998, [Online]. Dostupné z: https://www.vmware.com/pdf/esx_datasheet.pdf.

[46] VMware, „The Architecture of VMware ESXi", s. 10, 2006.

[47] A. Palo, „VMware Announces Support for 64-bit Computing", *web.archive.org*, dub. 19, 2004. https://web.archive.org/web/20090702000340/http:/www.vmware.com/company/news/releases/64bit.html (viděno dub. 27, 2020).

[48] D. M. F. Mattos, L. H. G. Ferraz, L. H. M. K. Costa, a O. C. M. B. Duarte, „Virtual Network Performance Evaluation for Future Internet Architectures", *JETWI*, roč. 4, č. 4, s. 304–314, lis. 2012, doi: 10.4304/jetwi.4.4.304-314.

[49] „What is Open Virtualization Format (OVF)? - Definition from Techopedia", *Techopedia.com*, srp. 18, 2011. https://www.techopedia.com/definition/4518/open-virtualization-format-ovf (viděno dub. 27, 2020).

[50] F. Tim, Twitter, a LinkedIn, „What IS an OVA File?", *Lifewire*, 11 2019. https://www.lifewire.com/ova-file-4144357 (viděno dub. 27, 2020).

[51] A. Mohanad, „Difference between OVA and OVF - vBlog", *vBlog*. https://sites.google.com/site/vblog77/notes/ovf-ova (viděno dub. 27, 2020).

[52] Š. Petr, „Zálohování ve virtualizovaném prostředí", *SystemOnLine.cz*, led. 2014. https://www.systemonline.cz/virtualizace/zalohovani-ve-virtualizovanem-prostredi.htm (viděno dub. 27, 2020).

[53] VMware, *Virtual Disk Format*. 2011.

[54] „ESXi Hardware Requirements", *ESXi Hardware*, kvě. 31, 2019. https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.esxi.install.doc/GUID-DEB8086A-306B-4239-BF76-E354679202FC.html (viděno dub. 27, 2020).

[55] „Download VMware vSphere Hypervisor for Free". https://my.vmware.com/en/web/vmware/evalcenter?p=free-esxi7&src=vmw_so_vex_dbori_1255 (viděno dub. 27, 2020).

[56] „Rufus - The Official Website (Download, New Releases)". https://rufus.ie/ (viděno dub. 27, 2020).

[57] „VMware Documentation". https://www.vmware.com/support/pubs/ (viděno dub. 27, 2020).

[58] „TechDocs". https://techdocs.broadcom.com/#symantec-security-software (viděno dub. 27, 2020).

[59] „Microsoft Documentation". https://docs.microsoft.com/en-us/ (viděno dub. 27, 2020).

[60] „The Official AnyBurn Website". http://www.anyburn.com/ (viděno dub. 27, 2020).

[61] „WinRAR download free and support: WinRAR". https://www.win-rar.com/start.html?&L=0 (viděno dub. 27, 2020).

[62] hajeklu, „hajeklu/Autounattend", dub. 22, 2020. https://github.com/hajeklu/Autounattend (viděno dub. 27, 2020).

[63] „How to Create and Deploy a Managed Software Delivery Policy", pro. 04, 2017. https://knowledge.broadcom.com/external/article/179840/how-to-create-and-deploy-a-managed-softw.html (viděno dub. 27, 2020).