

AC

Migrace Active Directory ve Třineckých železárnách

ZÁKAZNÍK STRUČNĚ

Třinecké železárný, kterým místní neřeknou jinak než Werk, patří k průmyslovým podnikům s nejdelší tradicí hutní výroby v České republice. Dnes významný podnik s uzavřeným hutním výrobním cyklem byl založen v roce 1839 Těšínskou komorou, kterou v té době vlastnil arcivévoda Karel Habsburský.

**TŘINECKÉ ŽELEZÁRNÝ**

OBDOBÍ REALIZACE

srpen - říjen 2017

„S přechodem Active Directory, souborových služeb a dalších částí infrastruktury na vyšší verzi operačního systému Windows Server 2016 se nám podařilo mimo jiné zvýšit efektivitu správy, zlepšit bezpečnost a současně eliminovat dopady ukončení podpory stávající verze operačního systému.“

Ing. Marian Rusina, MBA
vedoucí odboru FI - Informatika a telekomunikace

Výchozí situace a cíle projektu

Historie projektu se začala psát v roce 2008. Tehdy začala rychle se rozrůstající skupina Třinecké železárný - Moravia Steel pocítovat potřebu sjednotit nesourodé IT prostředí 20 firem v 5 lokalitách, čítající přes 3 000 koncových stanic a více než 4 000 uživatelských účtů, 7 oddělených AD domén, přes 20 jednotlivých Novell NDS adresářových služeb, v různých verzích...

Výstupem projektu byla konsolidace do jediné Active Directory domény při zachování decentralizovaného modelu správy, migrace souborových služeb (z Novell souborových služeb). Sjednocení názvů (zavedení jmenné konvence), změna statických IP adres na dynamické a nasazení GPO politik, sjednocení jmenného prostoru DNS mělo pozitivní dopad do správy koncových stanic.

Na konci roku 2016 bylo zřejmé, že s blížícím se ukončením podpory operačního systému Microsoft Windows Server 2008 SP2 ze strany výrobce (ohlášené datum 14. ledna 2020) je třeba začít připravovat přechod na aktuální verzi - Windows Server 2016. Stávající OS byl na konci životního cyklu, takže nově nasazované aplikace by bylo nutné po dvou letech upgradovat.

PŘÍNOSY

- Přejít na nejnovější verzi serverového OS
- Nové souborové služby s odolností vůči výpadku
- Interní certifikační autorita, PKI
- V.I.P. koncové stanice šifrovány technologií BitLocker
- Centrální služba DHCP s vysokou dostupností

POUŽITÉ TECHNOLOGIE

Microsoft Active Directory Directory Services (AD DS)

Microsoft Active Directory Certificate Services (AD CS)

Microsoft Failover Cluster (MSFC) Microsoft BitLocker

Microsoft IP address management (IPAM)

Microsoft Distributed File System (DFS)

Zároveň byl stanoven požadavek neprovádět jen prostý upgrade, ale využít nové vlastnosti OS Windows Server 2016, které zlepšují užitečnou hodnotu řešení, pomohou zvýšit efektivitu správy i úroveň bezpečnosti, a celkově zkvalitnit poskytované služby. Nasazení a konfiguraci těchto nových vlastností je efektivní provést souběžně s upgrade, v rámci realizace celkových změn.

Popis řešení

Než se takřikajíc „koplo do země“, byla na počátku roku 2017 vypracována studie přechodu na Windows Server 2016 s cílem popsat všechny plánované změny a provést rozdělení do etap. Vlastní realizace byla zahájena v srpnu 2017. Realizace probíhala paralelně ve dvou IT prostředích: celo-železárenská síť a technologická síť. Etapa Active Directory zahrnovala nahrazení doménových řadičů (včetně vzdálených lokalit), upgrade replikačního mechanismu SYSVOL, nasazení selektivní politiky hesel, využití bezpečnostních prvků nového operačního systému. V etapě souborové služby byl vytvořen nový jmenný prostor a vybudován MS Failover Cluster pro zajištění vysoké dostupnosti. Postupně došlo k migraci 7 TB souborových dat do nového úložiště. V etapě DHCP byly využity nové vlastnosti OS Windows Server 2016 k vytvoření vysoce dostupné služby v režimu Active-Standby s přesahem do vzdálených lokalit. Zároveň díky službě IPAM byla zachována autonomie správy DHCP pro administrátory vzdálených poboček. V rámci etapy PKI byla nasazena interní certifikační autorita na bázi MS Active Directory Certificate Services, vytvořeny procesní postupy pro správu CA, nasazeno šifrování koncových stanic technologií BitLocker a související úpravy v AD.

