**Požadavky na funkcionalitu školní doménové sítě, práva uživatelů, GPO, VLAN…**

**AD uživatelé a počítače**

* Rozdělení do OU (zak, ucitel, eko, jidelna, host) – dle požadavků školy nebo tohoto schématu
* OU odpovídá také uživatelským skupinám
* Skupiny mají rozdílný přístup k prostředkům sítě (sdílené složky, tiskárny atd.), například podle tohoto modelu:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Domain admin** | **Ucitel** | **Zak** | **Eko** | **SJ** | **Host** |
| **VLAN1** | **ano** | **ano** | **ano** | **ano** | **ano** | **ne** |
| **Sdílené složky doménových uživatelů** |  |  |  |  |  |  |
| výuka | Ano (r/w) | Ano (r) | Ano (r) |  |  |  |
| úkoly | Ano (r/w) | Ano (r/w) | Ano (r) |  |  |  |
| trh | Ano (r/w) | Ano (r/w) |  |  |  |  |
| Foto archiv školy | Ano (r/w) | Ano (r/w) |  |  |  |  |
| Sborovna | Ano (r/w) | Ano (r/w) |  |  |  |  |
|  |  |  |  |  |  |  |
| **Složky pro zálohy aplikací** |  |  |  |  |  |  |
| Zálohy účto, evidence majetku, faktury… | Ano (r/w) |  |  | Ano (r/w) |  |  |
| Zálohy jídelny | Ano (r/w) |  |  |  | Ano (r/w) |  |
| Zálohy doménových profilů a domovských adresářů | Ano (r/w) |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **VLAN2** |  |  |  |  |  |  |
| Internet pro hosty a soukromé učitelské telefony |  |  |  |  |  |  |
| **VLAN3** |  |  |  |  |  |  |
| Zálohování - replikace a archivace VM |  |  |  |  |  |  |
| **VLAN4** |  |  |  |  |  |  |
| Management Virtuálního clusteru |  |  |  |  |  |  |
| **VLAN5** |  |  |  |  |  |  |
| Zabezpečovačka, vstupy |  |  |  |  |  |  |
| IP kamery |  |  |  |  |  |  |
| **VLAN6** |  |  |  |  |  |  |
| Tiskárny (vidí pouze print server, přístupy dle AD) |  |  |  |  |  |  |
| **VLAN7** |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| **Jiné služby** |  |  |  |  |  |  |
| VPN | **Ano** | **Ano** | **ne** | **Ano** | **Ano** | **ne** |
| Školní mail | **Ano** | **Ano** | **ne** | **Ano** | **Ano** | **ne** |
|  |  |  |  |  |  |  |

* Všichni uživatelé mají cestovní profily s vyloučením složek Desktop, Documents a Appdata, které jsou mapovány přímo ze serveru (bez použití služby offline souborů). Tyto složky jsou zároveň podsložkami domovského adresáře uživatele, který se připojuje jako síťový disk pod písmenem H:
* Další síťové disky se připojují takto:
  + S: Sborovna - obsahuje důležité dokumenty školy (kurikulární dokumenty – ŠVP, uč. Plány…) a je sdílena všem učitelům
  + Výuka (V:) - obsahuje instalace i instalační média výukového SW, celá složka je sdílená pro čtení, žáci i učitelé z ní spouštějí výukový SW
  + Úkoly (U:) - je sdílená žákům pro čtení a učitelům pro čtení/zápis. Jejím prostřednictvím jsou žákům předávány i objemnější materiály a úkoly, vzorové dokumenty, odkazy na webové stránky, ankety apod…
  + Trh (T:) - Přístupná pouze učitelům (čtení i zápis) jako úložiště výukových materiálů, prezentací, audio a videomateriálů.
  + Foto a video archiv školy (F:) - Foto a video galerie všech školních akcí, přístupná pouze učitelům, do aktuálního roku lze zapisovat, všechny starší roky jsou pouze pro čtení
  + Install (I:) – Instalační média všech nevýukových programů, databanka scriptů, postupů, návodů, licenčních klíčů atd. přístupno pouze pro domain admins
* Tvorba uživatelských účtů
  + Hromadná – import bude probíhat powershellovým skriptem z excelového sešitu, který bude obsahovat sloupce jméno, příjmení a ročník žáka, skript přiřadí adekvátní OU, skupinu i expiraci účtu (u prvňáčků na 11 let, 2.r. na 10, 3.r na 9 atd.) Žáci budou do AD hromadně zaváděni na začátku každého školního roku (bude se jednat o žáky prvních tříd). Návrh uživatelského jména a ostatních položek, které budou předávány do Ad bude součástí implementace.
  + Žákovská data budou kvótována
    - Maximální velikost všech žákem vytvořených dat na serveru (cestovní profil + Home directory) na 1GB
  + Data učitelů budou kvótována
    - Maximální velikost učitelova Home directory = 20GB
    - Veškeré další složky umožňující učitelům zápis velkých objemů dat (Sborovna, trh, úkoly) nebudou kvótována
  + Data správních zaměstnanců (šj, eko) nebudou kvótována
  + Data hostů vůbec nebudou ukládána na server. Jejich skupina slouží pouze ke zpřístupnění připojení k internetu.
* Práva uživatelů k počítačům
  + Žáci i učitelé jsou standardní uživatelé, doménoví administrátoři jsou na všech strojích v doméně i lokálními administrátory. Je možno provést elevaci práv pro konkrétní doménové uživatele zařazením do pracovní skupiny s právy administrátora na lokálních strojích
  + Doménoví administrátoři mají zaručen přístup k profilům i domovským adresářům všech uživatelů
* Údržba domény
  + Kromě hromadného importu uživatelů je vhodné řešit i hromadné mazání expirovaných uživatelských účtů a dat včetně detekce „osiřelých“ SID a úpravy přístupových práv
* Systémové zprávy
  + Na jeden mailový alias budou chodit veškeré systémové zprávy napříč všemi použitými technologiemi (doména, kvóty, HW i SW incidenty…) Pro tyto účely může být zřízena zvláštní odesílací adresa (např. [report@nazevskoly.cz](mailto:report@nazevskoly.cz)).
* Zálohování a archivace
  + Zálohování celých virtuálních strojů bude nastaveno jako plně automatické, podle požadavků školy, případně podle tohoto schématu:
    - Kritické aplikace (účetnictví, majetek, strava, kurikulární a jiné důležité školní dokumenty) – denně – v nočních hodinách, případně alespoň mimo pracovní dobu
    - Běžné servery (doménové, zálohovací, webové, učitelská data, úložiště s výukovými materiály, foto a video materiály) – týdně – o víkendech
    - Servery s nízkou fluktuací dat (žákovské, archivy) – měsíčně
  + Zálohování virtuálních strojů bude probíhat po vyhrazené VLAN na úložiště, které nebude ze zbytku sítě přístupné (ochrana před ransomware)
  + Data vyžadující archivaci budou archivována automaticky podle školou požadovaného časového schématu a množství, minimálně se bude jednat o data účetní, stravovací, evidence majetku, pokladny, podací deníky atd. Tyto archivy budou ukládány v úložišti přístupném z lokální sítě