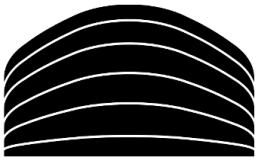
Koncepce infrastruktury



ICT NTK

Terminologie

“vysoká dostupnost” Systém je chráněn proti neočekávanému výpadku zdvojením nebo jiným druhem redundance na všech úrovních. Obnovení vysoké dostupnosti po výpadku může vyžadovat zásah obsluhy.

“zvýšená dostupnost” Systém je zajištěn jiným systémem v režimu vysoké dostupnosti tak, aby se automaticky zotavil z výpadku. Obnovení zvýšené dostupnosti může vyžadovat zásah obsluhy.

“běžná dostupnost” Systém není zajištěn proti výpadku. Každý výpadek vyžaduje nápravu ze strany obsluhy.

Logické celky

V infrastruktuře sledujeme následující logické celky:

Základní systémy

Základní systémy jsou naprosto kritické. Jejich nefunkčnost narušuje primární funkce NTK. Proto jsou, až na výjimky, provozovány v režimu vysoké dostupnosti.

Sítě

Konektivita Připojení počítačové sítě NTK k Internetu je zajištěno pomocí dvou rovnocenných optických linek přes akademickou síť sdružení CESNET.

Firewall Rozhraním mezi vnitřní sítí NTK a Internetem je hardwarový firewall. Tento firewall také odděluje jednotlivé zóny vnitřní sítě.

Přepínače V budově je, kromě vybavení serverovny, nainstalováno množství dalších zařízení, jako jsou kamery, tiskárny, terminály, kiosky, vyvolávací systém, stanice zaměstnanců, informační zobrazovače a bezdrátové přístupové body.

Pro účely těchto dalších zařízení se v každém patře nachází několik rozvoden, ve kterých jsou nainstalovány směrovače. Síť tvoří strom s kořenem v hlavním směrovači / přepínači v serverovně.

Přímo do centrálních přepínačů jsou také vysokokapacitně připojeny přepínače pro provoz vlastního datového centra.

Linky mezi přepínači jsou alespoň zdvojené a tudíž mají vysokou dostupnost. Přepínače samotné operují v tzv. stozích a preferované zapojení zdvojených linek je do dvou různých fyzických zařízení.

Systém autentizace koncových zařízení Zařízení připojená do patrových přepínačů musí být autentizována. V případě trvalých instalací, jako jsou například servery či kamery, je na daných portech nastavena fixní VLAN, jinak je použita autentizace pomocí hardwarových adres nebo pomocí vhodného autentizačního protokolu.

Zejména pro stanice a přenosná zařízení zaměstnanců je použit protokol pro autentizaci pomocí centrální databáze (aktuálně RADIUS). Různým zařízením je takto přiděleno členství v patřičných zónách pomocí VLAN.

Systém pro přidělování adres Ve většině případů jsou adresy klientským zařízením přidělovány pomocí protokolu DHCP na základě centrální konfigurace.

Systém překladu doménových jmen Překlad doménových jmen je zajištěn pomocí protokolu DNS. Jmenné servery pro domény ve vlastnictví NTK, tedy zejména `ntkcz.cz` a `techlib.cz` jsou umístěny přímo v síti NTK. Tyto zóny jsou také replikovány na jmenné servery CESNETu, které jsou vedené jako sekundární.

Doména `ntkcz.cz` je určena pouze pro interní použití. Doména `techlib.cz` pak pro veřejně dostupné služby. Pokud má zařízení název v doméně `techlib.cz`, musí mít i název v doméně `ntkcz.cz`. Tento název nemusí být shodný.

Systém řízení bezdrátové sítě Kromě pevné sítě disponuje budova NTK i sítí bezdrátovou. Ta je řízena centrálně pomocí zařízení instalovaných v serverovně. Jednotlivé přístupové body pak jednají koordinovaně.

Klientská zařízení jsou autentizována a různými způsoby rozdělena do patřičných zón. Zejména se jedná o zónu pro zaměstnance, zónu pro čtenáře a zónu pro uživatele ze sítě Eduroam.

Provozní databáze identit

Veškeré identity se kterými infrastruktura pracuje jsou uloženy v jednotné databázi a replikovány do dalších systémů. Jedním z těchto systémů je i provozní databáze identit realizovaná jako služba LDAP, sloužící k autentizaci a autorizaci klientů.

Služba LDAP je provozována v režimu zvýšené dostupnosti. Zotavení při výpadku je ponecháno na klientech, kteří musí zopakovat svůj pokus o autentizaci.

Úložné systémy

Úložné systémy poskytují úložný diskový prostor pro servery a databáze. Úložné systémy jsou odolné proti selhání hardware na úrovni jednotlivých disků, řadičů, ve výjimečných případech pak i na úrovni celých diskových polí.

Veškerá data systémů NTK jsou, pokud je to možné, uložena na některém z diskových polí s využitím technologie redundantních disků. Data základních systémů jsou navíc zrcadlena mezi více diskovými poli.

Databáze Oracle

Z historických důvodů je primární databáze identit uložena v databázi Oracle. Také se zde nachází data několika interních systémů.

Interní systémy

Interní systémy jsou využívány zaměstnanci NTK. Jejich nefunkčnost má dopad na vnitřní chod instituce, ale nemá zásadní dopad na schopnost NTK poskytovat běžné služby čtenářům.

Interní systémy jsou provozovány v režimu alespoň zvýšené dostupnosti.

Systém správy identit

Systém správy identit obhospodařuje databázi identit a zajišťuje replikaci uživatelských účtů a práv napříč ostatními systémy. Při výpadku není možné provádět registrace a změny uživatelských účtů.

Zálohovací řešení

Zálohovány jsou nejen databáze a datové soubory, ale i konfigurace serverů a dalších zařízení, například síťových prvků. Z důvodu rychlé obnovy jsou běžné provozní zálohy uloženy ve virtuální páskové knihovně, odkud jsou v případě potřeby delšího skladování archivovány na skutečné magnetické pásky. Retenční politika je specifická pro každý systém.

Obecně platí, že je možné všechny systémy spolehlivě obnovit ze záloh. V případě že tomu tak není, musí být ICT schopno systém v případě potřeby rychle zrekonstruovat.

Virtualizace

Virtualizace je zajištěna clusterem serverů, kdy při výpadku některého z nich dojde k restartu postižených virtuálních serverů na jiném fyzickém serveru, čímž je zajištěna zvýšená dostupnost těchto virtuálních severů a služeb na nich provozovaných.

Kromě provozu ostatních interních systémů, jako je například groupwarové řešení či systém sítového tisku, slouží virtualizační cluster především k provozu elektronických služeb knihovny, jako je knihovní katalog, rezervační a platební systém, vyhledávání či webová prezentace.

Virtualizace pro správu

Podpůrné systémy využívané zejména oddělením ICT jsou provozovány na samostatném serveru s běžnou dostupností.

Jedná se zejména o dohledový systém, systémy pro centrální správu a konfiguraci a knowledge base a issue tracking systém.

Systémy správy budovy

Tyto systémy zajišťuji provoz budovy jako celku (jde zejména o ovládání přístupu, zabezpečovací systém, systém měření a regulace a kamerový systém). ICT NTK zajišťuje provoz serverové infrastruktury těchto systémů v režimu zvýšené až vysoké dostupnosti. Detailní informace o systémech provozu budovy překračují rámec tohoto dokumentu.

Elektrická síť

UPS

Serverovna i jednotlivé rozvodny jsou jištěny pomocí UPS systémů na bázi baterií či fyzické setrvačnosti. Tyto systémy zaručí dočasné napájení v případě krátkého výpadku elektrické rozvodné sítě.

Diesel agregát

Diesel agregát dokáže nahradit elektrickou rozvodnou síť v případě delšího výpadku a zaručit tak setrvalý chod infrastruktury i v krizových situacích.

Obecná pravidla

Svobodný software

Svobodný software je preferovaný zejména pro svou praktičnost.

- Bývá dobře zdokumentovaný.
- Je běžně možné ho otestovat a zhodnotit před nákupem.
- Bývá široce používaný, řešení obtíží tak lze velmi často dohledat v diskuzích na Internetu, což snižuje až eliminuje náklady na podporu.
- V případě potřeby je možné ho modifikovat.
- Bývá integrovatelný do zbytku infrastruktury.
- Licenční náklady bývají nízké či žádné, což obecně snižuje náklady na ICT.
- Díky vysoké míře standardizace a liberálnímu přístupu k autorskoprávním otázkám a patentům nehrozí tzv. vendor lock-in.

Deklarativní centrální správa

Centrální správa infrastruktury umožňuje vytvoření pravidel a politik, které popisují stav konfigurace platformy. Koncová zařízení (například servery, pracovní stanice, síťové prvky a specializovaná zařízení) by měla tyto politiky aplikovat, a to ať už jde o změny konfigurace či instalace nových funkcí).

Deklarativní konfigurace je současně dokumentací aktuálního stavu a navíc umožňuje konzistentně provádět rozsáhlé změny a ověřovat jejich provedení.

Infrastruktura pod dohledem

Každý prvek infrastruktury je zanesen v dohledovém systému. Je sledován jeho stav a kondice na té úrovni, na jaké je prvek schopen tyto informace poskytovat, minimálně však na úrovni informace o základní funkčnosti či nefunkčnosti. V případě zjištění problému tento systém okamžitě upozorní správce daného prvku.

Porušení koncepce

Aktuálně evidujeme následující porušení koncepce:

Databáze Oracle a MS SQL

Databáze Oracle a MS SQL jsou provozovány v pouze režimu běžné dostupnosti, jelikož jsou umístěny přímo na fyzických serverech a neoperují v clusteru.

Důvodem je příliš vysoká cena za licence potřebné pro bezpečnější provoz. Bylo by totiž nutné licencovat všechny procesory, na kterých databáze může eventuálně běžet.

Důsledkem tohoto porušení je nutnost přezónování úložiště v případě havárie tohoto fyzického serveru. Z toho plyne, že havárie bude vyžadovat zásah obsluhy pro obnovení provozu a tudíž výrazné narušení běžného provozu.