Technická specifikace projektu

Tento dokument popisuje technické požadavky, které je nezbytné nabízeným řešením splnit. Všechny technické požadavky jsou povinné, vyjma těch, které jsou označeny jako volitelné měřitelné požadavky. Požadavky jsou minimální a nesplnění jakéhokoliv povinného požadavku povede k vyřazení nabídky Dodavatele. Volitelné měřitelné požadavky budou bodově ohodnoceny při jejich splnění či nesplnění.

1. Výpočetní servery

Jedná se o rozšíření stávající farmy využívající virtualizační technologii VMware vSphere/vCenter a operační systémy z rodiny Microsoft Windows. Zadavatel nemá technologickou preferenci dodávané procesorové platformy. Nutná je kompatibilita s x86_64 prostředím a dostupná informace o kompatibilitě na stránkách VMware: https://www.vmware.com/resources/compatibility/search.php.

Na výše uvedených stránkách VMware musí být explicitně uveden:

- model nabízeného serveru v nabízené verzi,
- modelová řada nabízených procesorů,
- podpora pro vSphere (ESXI) ve verzi 8.

Velký výpočetní server

- Montáž do standardního 19“ racku o maximální výšce 2 RU.
- Nejméně 2 CPU, každé o 32 jádrech na minimální frekvenci na všech jádrech 3.1Ghz při zpracování x86_64 instrukcí (požadavek je stanoven s ohledem na licenční omezení používaného software).
- Nejméně 16 ks 128GB DDR4 nebo DDR5 RAM modulů o základní frekvenci nejméně 3200Mhz s podporou ECC, každý paměťový kanál musí být osazen nejméně jedním modulem, všechny paměťové moduly musí být identické. Pro dosažení ideální prostupnosti RAM je požadováno, aby Dodavatel dodal takové řešení, které bude mít v každém paměťovém kanálu CPU alespoň jeden modul RAM. Zadavatel nepřipouští osazení RAM ve kterém nebude splněna tato podmínka.
- Nejméně 32 slotů na paměti RAM z důvodu rozšiřitelnosti platformy. Podpora minimálně 10TB RAM per server. Zadavatel se obává možné nedostatečné velikosti RAM v budoucnu. Požaduje takové řešení, které bude rozšiřitelné na úroveň, kde tento limit nebude představovat omezení. Tento požadavek má Zadavatel i s ohledem na to, že výpočetní servery jsou provozovány často i 10 let.
- Nejméně dvě dvouportové síťové karty o rychlosti právě 10/25 Gbps nebo 25/100 Gbps osazené patřičnými transceivery.
- Volitelně dvě jednoportové FC HBA o rychlosti nejméně 32Gbps osazené SFP moduly (pouze v případě volby FC diskového pole).
- Nejméně 2 SSD disky o velikosti 240GB v Raid 1 poli.
- Nejméně jeden diskový řadič pro připojení 24 SFF disků včetně příslušné kabeláže. 24 SFF disků je požadováno pro umožnění instalování hybridních kombinací HDD a SSD.
- HW management serveru s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence.

- Možnost rozšíření interního managementu o update serveru online (z OS) i bez nutnosti instalace dalšího nástroje pro správu, možnost bootu a instalace z interní SD karty.

- Podpora Silicon Root Of Trust, Secure Boot a Chain Of Trust (kontrola zabezpečení celého výrobního řetězce), TPM 2.0, RedFish API.
- Nejméně 2 za chodu vyměnitelné napájecí zdroje s platinovou účinností. Server musí být v dodávané konfiguraci schopen fungovat na jeden napájecí zdroj s tím, že jeho zátěž nesmí překročit 75%.
- Licence na Microsoft Windows Datacenter 2019 na všechna CPU jádra.
- Licence VMware vSphere Enterpise Plus na všechna CPU jádra.
- Zajištění podpory výrobce minimálně 9x5 NBD v pracovních dnech se čtyřhodinovou reakční dobou v místě instalace na 5 let.

Malý výpočetní server

- Montáž do standardního 19“ racku o maximální výšce 2 RU.
- Nejméně 2 CPU, každé o 16 jádrech na minimální frekvenci na všech jádrech 3.3Ghz při zpracování x86_64 instrukcí (požadavek je stanoven s ohledem na licenční omezení používaného software).
- Nejméně 16 ks 32GB DDR4 nebo DDR5 RAM modulů o základní frekvenci nejméně 3200Mhz s podporou ECC, každý paměťový kanál musí být osazen nejméně jedním modulem, všechny paměťové moduly musí být identické. Pro dosažení ideální prostupnosti RAM je požadováno, aby Dodavatel dodal takové řešení, které bude mít v každém paměťovém kanálu CPU alespoň jeden modul RAM. Zadavatel nepřipouští osazení RAM ve kterém nebude splněna tato podmínka.
- Nejméně 32 slotů na paměti RAM z důvodu rozšiřitelnosti platformy. Podpora minimálně 10TB RAM per server. Zadavatel se obává možné nedostatečné velikosti RAM v budoucnu. Požaduje takové řešení, které bude rozšiřitelné na úroveň, kde tento limit nebude představovat omezení. Tento požadavek má Zadavatel i s ohledem na to, že výpočetní servery jsou provozovány často i 10 let.
- Nejméně dvě dvouportové síťové karty o rychlosti právě 10/25 Gbps nebo 25/100 Gbps osazené patřičnými transceivery.
- Volitelně dvě jednoportové FC HBA o rychlosti nejméně 32Gbps osazené SFP moduly (pouze v případě volby FC diskového pole).
- Nejméně 2 SSD disky o velikosti 240GB v Raid 1 poli.
- Nejméně jeden diskový řadič pro připojení 24 SFF disků včetně příslušné kabeláže. 24 SFF disků je požadováno pro umožnění instalování hybridních kombinací HDD a SSD.
- HW management serveru s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence.
- Možnost rozšíření interního managementu o update serveru online (z OS) i bez nutnosti instalace dalšího nástroje pro správu, možnost bootu a instalace z interní SD karty.
- Podpora Silicon Root Of Trust, Secure Boot a Chain Of Trust (kontrola zabezpečení celého výrobního řetězce), TPM 2.0, RedFish API.
- Nejméně 2 za chodu vyměnitelné napájecí zdroje s platinovou účinností. Server musí být v dodávané konfiguraci schopen fungovat na jeden napájecí zdroj s tím, že jeho zátěž nesmí překročit 75%.
- Licence na Microsoft Windows Datacenter 2019 na všechna CPU jádra.

- Licence VMware vSphere Enterpise Plus na všechna CPU jádra.
- Podpora výrobce minimálně 9x5 NBD v pracovních dnech se čtyřhodinovou reakční dobou v místě instalace na 5 let.

2. Bloková disková pole

Vždy dvě disková pole tvoří technologický celek pro virtualizační platformu VMware. Zadavatel plánuje synchronní replikaci v jedné lokalitě a to takovou, že budou obě disková pole zapisovatelná a čitelná současně. Technický koncept je popsán jako VMware non-uniform vMSC cluster. Nabízené datové úložiště bude nejméně dvou řadičové pole v režimu řadičů active-active, ALUA není dovolena. Mezi jednotlivými clustery diskových polí musí být funkční asynchronní replikace pomocí technologie postavené na přenosové vrstvě Ethernet. Zadavatel neomezuje použitý protokol. Mezi lokalitami nebude technicky možné použít technologii Fibre Channel.

Velké blokové diskové pole

- Minimální požadovaná kapacita je 140 TiB pro uložení dat uživatelského prostředí VMware vSphere.
- Datové úložiště musí podporovat použití protokolu NVMe pro interní operace včetně komunikace s případnými dalšími diskovými policemi. V IO cestě nesmí být použitý SAS nebo SATA protokol.
- Firmware respektive řídící OS řadičů pole musí být vyvíjený pro obsluhu flash modulů/SSD disků.
- Diskové pole musí být kompatibilní s platformou VMware vSphere 8 a vyšší. Zadavatel si ověří kompatibilitu prostřednictvím kontroly informací uvedených na stránkách výrobce VMware: https://www.vmware.com/resources/compatibility/search.php?deviceCategory=san
  s atributy:
  - ESXi 8.0,
  - NVMe.
- Disková úložiště musí být vybavena licencemi pro všechny požadované funkce systému a současně pro maximální dosažitelnou kapacitu nabízeného modelu. Požadavek se týká i budoucích funkcí systému. Zadavatel preferuje časově neomezenou licenci. Pokud je licence časově omezena, pak omezení nesmí být kratší, nežli sedm let.
- Řešení musí mít nativní připojení k síti SAN prostřednictvím protokolu Fibre Channel s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 32 Gbps. Alternativou je použití protokolu iSCSI s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 25 Gbps. Diskové pole musí být certifikováno pro VMware vSphere 7.0U3 vStorage APIs for Storage Awareness a NVMe-OF pro použitý protokol.
- Pro replikaci geograficky vzdálených datových úložišť budou vyhrazeny dva ethernetové porty o rychlosti 10/25Gbps nebo 100Gbps na každém z instalovaných řadičů.
- Diskové pole musí podporovat deduplikaci a kompresi dat. Výpočet poměru deduplikace a komprese je ponechán na Dodavateli. Na diskovém poli bude pouze virtualizační zátěž (VMware). Zdrojová data budou mít rozdílnou velikost bloku, nebudou šifrována ani komprimována. Při použití deduplikace a komprese k dosažení požadované čisté kapacity diskového pole, bude Dodavatel garantovat poměr deduplikace a komprese. Zadavatel bude po dodavateli požadovat ověření garance potvrzením přímo od výrobce. Garanci musí výrobce držet minimálně po dobu 5 let. Při nesplnění poměru deduplikace a komprese o více než-li 5% zajistí dodavatel patřičnou diskovou kapacitu pomocí dodávky dalších/větších diskových. Pokud pole nepodporuje kompresi a deduplikaci zároveň globálně nad všemi ukládanými daty

současně a nebo pokud zapnutá deduplikace nebo komprese snižuje výkon pole pod požadavky zadavatele, pak je nutné dodat celkovou požadovanou kapacitu bez započítání deduplikace a komprese. Do poměru deduplikace a komprese nelze započíst snapshoty a tenký provisioning. Požadavek na deduplikaci a kompresi je dán hlavně z pohledu budoucí rozšířitelnosti. Diskové pole, které nebude disponovat deduplikací a kompresí, bude při dalším rozšiřování méně efektivní. Farma virtuálních systémů je do jisté míry homogenní. Systém nepodporující deduplikaci a kompresi bude zbytečně spotřebovávat kapacitu při budoucím rozšíření. Kritérium je nastaveno tak, aby zvýhodnilo řešení s co možná nejefektivnější deduplikací a kompresí.

- Zadavatel požaduje funkcionalitu zabezpečeného snapshotu (neměnného, immutable) prostředky dodávaného blokového diskového úložiště. S takovým snapshotem není možno po nastavenou dobu nijak manipulovat (měnit, odstranit, modifikovat retenci) ani za použití nejvyšších administrátorských oprávnění v rámci daného diskového úložiště (ochrana proti zneužití administrátorských oprávnění).
- Zaplnění pole na 100% dostupné kapacity nesmí způsobit ztrátu přístupu k datům.
- Nabízené diskové pole nesmí obsahovat Single Point Of Failure tj.musí být odolné min.proti výpadku jedné komponenty typu řadič, zdroj, cache, ventilátor, HBA apod.
- Výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu pole.
- Řešení musí nabídnout mechanismus pro detekci a opravu poškozených dat způsobem, který je transparentní pro servery.
- Řešení musí podporovat šifrování dat pomocí standardních bezpečných algoritmů (např. AES-256 nebo silnější) a šifrovat všechna média podporovaná v zařízení. Šifrování dat nesmí ovlivnit výkon řešení. Šifrovací klíč musí být generován způsobem, který zabraňuje čtení dat z médií odebraných z pole. Pole musí dále podporovat ukládání šifrovacích klíčů na Key Management serveru Zadavatele.
- Součástí dodávky jsou technické, SW a licenční prostředky umožňující vzdálenou synchronní a asynchronní replikaci dat. Diskové pole musí být certifikováno pro ne-uniformní (non-uniform) vMSC VMware storage klastr s uvedením informace o podpoře na stránkách VMware (například články: 77061, 2134684, 51656, 2151070). Nelze použít diskové pole, kde vendor preferuje použití uniformního nad ne-uniformním VMware klastrem. Takto vytvořený geografický storage klastr musí poskytovat stejný volume (se stejným ID) pro operace čtení a zápisu na obou nabízených polích tvořících jednotný klastr.
- Řešení musí poskytovat úzkou integraci s virtualizační platformou poskytující analýzu kritických informací, funkcionality a dostupnosti celého řetězce od diskových úložišť až po úroveň konkrétních virtuálních serverů na platformě VMware vSphere. Nástroj musí zobrazovat přehledným grafickým způsobem rozložení zátěže od úrovně virtuálního serveru, přes využitý disk, datastore, hostitele až do úrovně použitého svazku a úložiště, ze kterého jsou konzumovány zdroje.
- Maximální výkon úložiště musí být dosažitelný se všemi funkcemi redukce dat, které jsou aktivní a funkční, bez ohledu na stupeň zaplnění fyzického prostoru daty. V případě, že společně se zaplněním daty dochází k redukci výkonu datového úložiště, je přípustná instalace většího datového prostoru nad uvedený minimální požadovaný garantovaný objem dat. Tento prostor může být využit pro kompenzaci ztráty výkonu datového úložiště z důvodu zaplnění daty.

- Požadovaný výkon úložiště při 100% random zátěži a poměru čtení/zápis 70%/30% a velikostí bloku 64 KiB je min. 100000 IOPS. Výkonnostní parametry musí být doloženy Dodavatelem autentickým snímkem obrazovky z oficiálního nástroje výrobce pro návrh diskových polí. Pokud Dodavatel tuto možnost nemá, musí prokázat výkon syntetickým testem v IT prostředí Zadavatele včetně zápůjčky kompletního řešení infrastruktury. Test bude probíhat nástrojem Iometer s profilem zadaným dle ZD.
- Maximální latence při použití zvoleného protokolu 0,75 ms (IOPS nad latenci 0,75 ms nelze do výkonu započítat).
- Dodavatel zajistí podporu výrobce 24x7 non stop s 15ti minutovou reakční dobou výrobce vzdáleně a doručením náhradního dílu následujícího pracovního dne v místě instalace, a to na dobu 5 let.

Střední blokové diskové pole

- Minimální požadovaná kapacita je 90 TiB pro uložení dat uživatelského prostředí VMware vSphere.
- Datové úložiště musí podporovat použití protokolu NVMe pro interní operace včetně komunikace s případnými dalšími diskovými policemi. V IO cestě nesmí být použitý SAS nebo SATA protokol.
- Firmware respektive řídící OS řadičů pole musí být vyvíjený pro obsluhu flash modulů/SSD disků.
- Disková úložiště musí být vybavena licencemi pro všechny požadované funkce systému a současně pro maximální dosažitelnou kapacitu nabízeného modelu. Požadavek se týká i budoucích funkcí systému. Zadavatel preferuje časově neomezenou licenci. Pokud je licence časově omezena, pak omezení nesmí být kratší, nežli sedm let.
- Řešení musí mít nativní připojení k síti SAN prostřednictvím protokolu Fibre Channel s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 32 Gbps. Alternativou je použití protokolu iSCSI s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 25 Gbps. Diskové pole musí být certifikováno pro VMware vSphere 7.0U3 vStorage APIs for Storage Awareness a NVMe-OF pro použitý protokol.
- Pro replikaci geograficky vzdálených datových úložišť budou vyhrazeny dva ethernetové porty o rychlosti 10/25Gbps na každém z instalovaných řadičů.
- Diskové pole musí podporovat deduplikaci a kompresi dat. Výpočet poměru deduplikace a komprese je ponechán na Dodavateli. Na diskovém poli bude pouze virtualizační zátěž (VMware). Zdrojová data budou mít rozdílnou velikost bloku, nebudou šifrována ani komprimována. Při použití deduplikace a komprese k dosažení požadované čisté kapacity diskového pole, bude Dodavatel garantovat poměr deduplikace a komprese. Zadavatel bude po dodavateli požadovat ověření garance potvrzením přímo od výrobce. Garanci musí výrobce držet minimálně po dobu 5 let. Při nesplnění poměru deduplikace a komprese o více než-li 5% zajistí dodavatel patřičnou diskovou kapacitu pomocí dodávky dalších/větších diskových. Pokud pole nepodporuje kompresi a deduplikaci zároveň globálně nad všemi ukládanými daty současně a nebo pokud zapnutá deduplikace nebo komprese snižuje výkon pole pod požadavky zadavatele, pak je nutné dodat celkovou požadovanou kapacitu bez započítání deduplikace a komprese. Do poměru deduplikace a komprese nelze započíst snapshoty a tenký provisioning. Požadavek na deduplikaci a kompresi je dán hlavně z pohledu budoucí rozšířitelnosti. Diskové pole, které nebude disponovat deduplikací a kompresí, bude při dalším rozšiřování méně efektivní. Farma virtuálních systémů je do jisté míry homogenní. Systém

nepodporující deduplikaci a kompresi bude zbytečně spotřebovávat kapacitu při budoucím rozšíření. Kritérium je nastaveno tak, aby zvýhodnilo řešení s co možná nejefektivnější deduplikací a kompresí.

- Zadavatel požaduje funkcionalitu zabezpečeného snapshotu (neměnného, immutable) prostředky dodávaného blokového diskového úložiště. S takovým snapshotem není možno po nastavenou dobu nijak manipulovat (měnit, odstranit, modifikovat retenci) ani za použití nejvyšších administrátorských oprávnění v rámci daného diskového úložiště (ochrana proti zneužití administrátorských oprávnění).
- Zaplnění pole na 100% dostupné kapacity nesmí způsobit ztrátu přístupu k datům.
- Nabízené diskové pole nesmí obsahovat Single Point Of Failure tj. musí být odolné min. proti výpadku jedné komponenty typu řadič, zdroj, cache, ventilátor, HBA apod.
- Výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu pole.
- Řešení musí nabídnout mechanismus pro detekci a opravu poškozených dat způsobem, který je transparentní pro servery.
- Řešení musí podporovat šifrování dat pomocí standardních bezpečných algoritmů (např. AES-256 nebo silnější) a šifrovat všechna média podporovaná v zařízení. Šifrování dat nesmí ovlivnit výkon řešení. Šifrovací klíč musí být generován způsobem, který zabraňuje čtení dat z médií odebraných z pole. Pole musí dále podporovat ukládání šifrovacích klíčů na Key Management serveru Zadavatele.
- Součástí dodávky jsou technické, SW a licenční prostředky umožňující vzdálenou synchronní a asynchronní replikaci dat. Diskové pole musí být certifikováno pro ne-uniformní (non-uniform) vMSC VMware storage klastr s uvedením informace o podpoře na stránkách VMware (například články: 77061, 2134684, 51656, 2151070). Nelze použít diskové pole, kde vendor preferuje použití uniformního nad ne-uniformním VMware klastrem. Takto vytvořený geografický storage klastr musí poskytovat stejný volume (se stejným ID) pro operace čtení a zápisu na obou nabízených polích tvořících jednotný klastr.
- Řešení musí poskytovat úzkou integraci s virtualizační platformou poskytující analýzu kritických informací, funkcionality a dostupnosti celého řetězce od diskových úložišť až po úroveň konkrétních virtuálních serverů na platformě VMware vSphere. Nástroj musí zobrazovat přehledným grafickým způsobem rozložení zátěže od úrovně virtuálního serveru, přes využitý disk, datastore, hostitele až do úrovně použitého svazku a úložiště, ze kterého jsou konzumovány zdroje.
- Maximální výkon úložiště musí být dosažitelný se všemi funkcemi redukce dat, které jsou aktivní a funkční, bez ohledu na stupeň zaplnění fyzického prostoru daty. V případě, že společně se zaplněním daty dochází k redukci výkonu datového úložiště, je přípustná instalace většího datového prostoru nad uvedený minimální požadovaný garantovaný objem dat. Tento prostor může být využit pro kompenzaci ztráty výkonu datového úložiště z důvodu zaplnění daty.
- Požadovaný výkon úložiště při 100% random zátěži a poměru čtení/zápis 70%/30% a velikostí bloku 64 KiB je min. 70 000 IOPS. Výkonnostní parametry musí být doloženy autentickým snímkem obrazovky z oficiálního nástroje výrobce pro návrh diskových polí. Pokud výrobce tuto možnost nemá, musí prokázat výkon syntetickým testem v prostředí Zadavatele včetně zápůjčky kompletního řešení infrastruktury. Test bude probíhat nástrojem Iometer s profilem zadaným dle ZD.

- Maximální latence při použití zvoleného protokolu 0,75 ms (IOPS nad latenci 0.75 ms nelze do výkonu započítat).
- Dodavatel zajistí podporu výrobce 24x7 non stop s 15ti minutovou reakční dobou výrobce vzdáleně a doručením náhradního dílu následujícího pracovního dne v místě instalace , a to na dobu 5 let.

Malé blokové diskové pole

- Minimální požadovaná kapacita je 20TiB pro uložení dat uživatelského prostředí VMware vSphere.
- Datové úložiště musí podporovat použití protokolu NVMe pro interní operace včetně komunikace s případnými dalšími diskovými policemi. V IO cestě nesmí být použitý SAS nebo SATA protokol.
- Firmware respektive řídící OS řadičů pole musí být vyvíjený pro obsluhu flash modulů/SSD disků.
- Disková úložiště musí být vybavena licencemi pro všechny požadované funkce systému a současně pro maximální dosažitelnou kapacitu nabízeného modelu. Požadavek se týká i budoucích funkcí systému. Zadavatel preferuje časově neomezenou licenci. Pokud je licence časově omezena, pak omezení nesmí být kratší, nežli sedm let.
- Řešení musí mít nativní připojení k síti SAN prostřednictvím protokolu Fibre Channel s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 32 Gbps. Alternativou je použití protokolu iSCSI s minimálním počtem portů 2 na každém z instalovaných řadičů a minimální propustností každého portu 25 Gbps. Diskové pole musí být certifikováno pro VMware vSphere 7.0U3 vStorage APIs for Storage Awareness a NVMe-OF pro použitý protokol.
- Pro replikaci geograficky vzdálených datových úložišť budou vyhrazeny dva ethernetové porty o rychlosti 10/25Gbps na každém z instalovaných řadičů.
- Diskové pole musí podporovat deduplikaci a kompresi dat. Výpočet poměru deduplikace a komprese je ponechán na Dodavateli. Na diskovém poli bude pouze virtualizační zátěž (VMware). Zdrojová data budou mít rozdílnou velikost bloku, nebudou šifrována ani komprimována. Při použití deduplikace a komprese k dosažení požadované čisté kapacity diskového pole, bude Dodavatel garantovat poměr deduplikace a komprese. Zadavatel bude po dodavateli požadovat ověření garance potvrzením přímo od výrobce. Garanci musí výrobce držet minimálně po dobu 5 let. Při nesplnění poměru deduplikace a komprese o více než-li 5% zajistí dodavatel patřičnou diskovou kapacitu pomocí dodávky dalších/větších diskových. Pokud pole nepodporuje kompresi a deduplikaci zároveň globálně nad všemi ukládanými daty současně a nebo pokud zapnutá deduplikace nebo komprese snižuje výkon pole pod požadavky zadavatele, pak je nutné dodat celkovou požadovanou kapacitu bez započítání deduplikace a komprese. Do poměru deduplikace a komprese nelze započíst snapshoty a tenký provisioning. Požadavek na deduplikaci a kompresi je dán hlavně z pohledu budoucí rozšířitelnosti. Diskové pole, které nebude disponovat deduplikací a kompresí, bude při dalším rozšiřování méně efektivní. Farma virtuálních systémů je do jisté míry homogenní. Systém nepodporující deduplikaci a kompresi bude zbytečně spotřebovávat kapacitu při budoucím rozšíření. Kritérium je nastaveno tak, aby zvýhodnilo řešení s co možná nejefektivnější deduplikací a kompresí.
- Zadavatel požaduje funkcionalitu zabezpečeného snapshotu (neměnného, immutable) prostředky dodávaného blokového diskového úložiště. S takovým snapshotem není možno po

nastavenou dobu nijak manipulovat (měnit, odstranit, modifikovat retenci) ani za použití nejvyšších administrátorských oprávnění v rámci daného diskového úložiště (ochrana proti zneužití administrátorských oprávnění).

- Zaplnění pole na 100% dostupné kapacity nesmí způsobit ztrátu přístupu k datům.
- Nabízené diskové pole nesmí obsahovat Single Point Of Failure tj. musí být odolné min. proti výpadku jedné komponenty typu řadič, zdroj, cache, ventilátor, HBA apod.
- Výpadek žádné komponenty včetně řadiče diskového pole nesmí způsobit pokles požadovaného výkonu pole.
- Řešení musí nabídnout mechanismus pro detekci a opravu poškozených dat způsobem, který je transparentní pro servery.
- Řešení musí podporovat šifrování dat pomocí standardních bezpečných algoritmů (např. AES-256 nebo silnější) a šifrovat všechna média podporovaná v zařízení. Šifrování dat nesmí ovlivnit výkon řešení. Šifrovací klíč musí být generován způsobem, který zabraňuje čtení dat z médií odebraných z pole. Pole musí dále podporovat ukládání šifrovacích klíčů na Key Management serveru Zadavatele.
- Součástí dodávky jsou technické, SW a licenční prostředky umožňující vzdálenou synchronní a asynchronní replikaci dat. Diskové pole musí být certifikováno pro ne-uniformní (non-uniform) vMSC VMware storage klastr s uvedením informace o podpoře na stránkách VMware (například články: 77061, 2134684, 51656, 2151070). Nelze použít diskové pole, kde vendor preferuje použití uniformního nad ne-uniformním VMware klastrem. Takto vytvořený geografický storage klastr musí poskytovat stejný volume (se stejným ID) pro operace čtení a zápisu na obou nabízených polích tvořících jednotný klastr.
- Řešení musí poskytovat úzkou integraci s virtualizační platformou poskytující analýzu kritických informací, funkcionality a dostupnosti celého řetězce od diskových úložišť až po úroveň konkrétních virtuálních serverů na platformě VMware vSphere. Nástroj musí zobrazovat přehledným grafickým způsobem rozložení zátěže od úrovně virtuálního serveru, přes využitý disk, datastore, hostitele až do úrovně použitého svazku a úložiště, ze kterého jsou konzumovány zdroje.
- Maximální výkon úložiště musí být dosažitelný se všemi funkcemi redukce dat, které jsou aktivní a funkční, bez ohledu na stupeň zaplnění fyzického prostoru daty. V případě, že společně se zaplněním daty dochází k redukci výkonu datového úložiště, je přípustná instalace většího datového prostoru nad uvedený minimální požadovaný garantovaný objem dat. Tento prostor může být využit pro kompenzaci ztráty výkonu datového úložiště z důvodu zaplnění daty.
- Požadovaný výkon úložiště při 100% random zátěži a poměru čtení/zápis 70%/30% a velikostí bloku 64 KiB je min. 70 000 IOPS. Výkonnostní parametry musí být doloženy autentickým snímkem obrazovky z oficiálního nástroje výrobce pro návrh diskových polí. Pokud výrobce tuto možnost nemá, musí prokázat výkon syntetickým testem v prostředí Zadavatele včetně zápůjčky kompletního řešení infrastruktury. Test bude probíhat nástrojem Iometer s profilem zadaným dle ZD.
- Maximální latence při použití zvoleného protokolu 0,75 ms (IOPS nad latenci 0,75 ms nelze do výkonu započítat).
- Dodavatel zajistí podporu výrobce 24x7 non stop s 15ti minutovou reakční dobou výrobce vzdáleně a doručením náhradního dílu následujícího pracovního dne v místě instalace, a to na dobu 5 let.

3. Diskové pole pro nestrukturovaná data

- Montáž do standardního 19“ racku o maximální výšce 10 RU.
- Scale out architektura s nejméně 4-mi identickými uzly postavená na principu redundance médií pomocí technologie erasure coding. Řešení musí být odolné na výpadek jednoho hardware uzlu a nejméně 2 médií-disků z každého uzlu. Požadavek na nejméně 4 uzly je dán požadavkem na užití technologie erasure coding. EC schéma je při použití menšího počtu uzlů méně efektivní (hrubá vs užitná kapacita). Zadavatel má zájem o co možná nejvyšší efektivitu ec schématu.
- Diskové pole bude využívat protokol NFS v4.1 a také protokol SMB v3.
- Řešení musí podporovat protokol S3 pro přesouvání záloh a musí disponovat vlastním REST API pro kompletní správu pole a diskového prostoru z aplikace.
- Diskové pole musí disponovat technologií pro replikaci mezi dvěma diskovými poli na úrovni souborové vrstvy. Replikace musí probíhat kontinuálně. Přípustná je jak asynchronní, tak synchronní replikace.
- Řešení musí být schopno získat identitu a strom přístupových oprávnění na základě čtení uživatelského stromu z Microsoft Active Directory a Linux LDAP. Řešení musí umět používat obě funkce, nikoliv však zároveň.
- Řešení musí být vybaveno přístupovými seznamy a to zejména pro protokol NFS. Bezpečnost musí být vázána k souboru a k uživatelské identitě přistupujícího uživatele. Nejméně musí být rozpoznány příznaky čtení, zápis a řízení oprávnění k souboru.
- Řešení musí být prezentováno uživatelům jako jeden name space. Řešení musí mít integrovaný load balancer, tak aby zátěž byla mezi uzly rozkládána rovnoměrně.
- Řešení musí podporovat snapshoty a to tak, že snapshot vytvoří zámek na dané souborové struktuře a následně nebude možné se soubory manipulovat. V kombinaci se zálohovacím software musí tato funkce vytvářet nepozměnitelný repozitář záloh.
- Řešení musí podporovat šifrování dat (data at rest encryption). Požadavek je alespoň na šifrování pomocí AES-256. Šifrování nesmí být založeno na hardware, pro případ potřeby migrace mezi různými hardwarovými platformami. Řešení musí chránit média i poté co byla vyřazena z provozu a nedopatřením se vyřazené médium dostane do nesprávných rukou. Řešení musí obsahovat interní transparentní správu klíčů. Řešení musí obsahovat mechanismus pro efektivní rotaci šifrovacích klíčů.
- Uložená data budou komprimována a potenciálně i šifrována. Funkce deduplikace a komprese není požadována. Deduplikační a kompresní poměr nelze započíst do výpočtu celkové kapacity. Požadovaná čistá kapacita je nejméně 750 TB.
- Požadovanou kapacitu bude možné využít celou tj. pokud výrobce doporučuje využití např. max.do 90% dodané kapacity, pak zadavatel požaduje navýšit dodanou kapacitu.
- Diskové pole bude sloužit pro paralelní přístup systémů i uživatelů. Diskové pole musí být schopno zároveň komunikovat s nejméně 2000 uživateli a 200 systémy (NFSv4.1). Diskové pole musí disponovat nejméně 24ti CPU jádry o základní frekvenci nejméně 2 Ghz. Zadavatel spočítal počet uživatelů na jedno CPU jádro a vychází ze standardních doporučení pro budování scale-out diskových polí. Dodavatel musí v návaznosti na požadavky zadavatele a s přihlédnutím k nabízenému řešení vyhodnotit, zdali bude stačit nasadit Zadavatelem uvedený minimální počet CPU jader, anebo použije počet vyšší.
- Diskové pole musí disponovat nejméně 4 x 10 nebo 25 GbE frontend porty a 4 x 10 nebo 25GbE backend porty. Porty lze v případě sdílení libovolně kombinovat. Celkový nejmenší počet portů je 12 ks. Každý uzel musí disponovat nejméně dvěma porty.

- Diskové pole musí disponovat nejméně 50 000 IOPS (NFSv4.1). Celkový výkon pro čtení musí být nejméně 3.05 GB za vteřinu a celkový výkon pro zápis nejméně 3.05 GB za vteřinu. Jedno spojení musí být schopno zapisovat rychlostí nejméně 1.05 GB za vteřinu a číst rychlostí 1.05 GB za vteřinu. Výkon musí být možné dosáhnout na 100% požadované kapacity.
- V případě potřeby růstu kapacity musí být možné navýšení nejméně na 200% úvodní kapacity (1500TB). Navýšení musí být provedeno formou scale-out pomocí přidávání identických nodů. V plánu je rozšíření na více než dvojnásobek kapacity. Rozšířené pole pak musí splňovat následující požadavky: 100 000 IOPS (NFSv4.1), celkový výkon pro čtení 6.1GB za vteřinu a výkon pro zápis nejméně 6.1GB za vteřinu. Pole po rozšíření musí dále splňovat požadavek na možnost rozšíření o nejméně dalších 200% diskové kapacity.
- Diskové pole musí umožnit konsolidaci dvou polí do jednoho clusteru za dodržení podmínek pro rozšíření na 200% kapacity stanovených v bodě výše.
- Dodavatel zajistí podporu výrobce 9x5 NBD v pracovních dnech s reakcí následující pracovní den v místě instalace, a to na dobu 5 let.

4. Zálohovací server a infrastrukturní server

- Montáž do standardního 19“ racku o maximální výšce 2 RU.
- Nejméně 2 CPU, každé o 16 jádrech na minimální frekvenci na všech jádrech 3.1Ghz při zpracování instrukcí x86_64. Server bude sloužit jako management platforma pro technologie datového centra. Minimální požadavek na výkon CPU je dán s ohledem na očekávaný overhead zálohovací software a technologií pro správu datového centra. Zadavatel vycházel z doporučení výrobců pro software pro management platformy (VMware a náhodně vybraný zálohovací software)
- Nejméně 8 ks 32GB DDR4 nebo DDR5 RAM modulů o základní frekvenci nejméně 3200Mhz s podporou ECC. Minimílní kapacita RAM je definována minimálními požadavky na kapacitu ze strany výrobců software pro management platformy (VMware a náhodně vybraný zálohovací software).
- 32 slotů na paměti RAM. Požadavek je dán skutečností, že Zadavatel potřebuje schopnost rozšířit RAM až na 1TB. Vychází to z provozní zkušenosti, kdy výrobci management platforem neustále stupňují své požadavky na využití operační paměti (například Veeam ONE apod.).
- Nejméně dvě dvouportové síťové karty o rychlosti 10/25 Gb nebo 100 Gb.
- Volitelně dvě jednoportové FC HBA o rychlosti nejméně 32Gbps (pouze v případě volby FC diskového pole).
- Nejméně 2 SSD disky o velikosti 240GB v Raid 1 poli.
- Nejméně jeden diskový řadič pro připojení 12 SFF disků včetně příslušné kabeláže. Nejméně 12 x 6TB HDD 7200 rpm SATA nebo SAS. Zadavatel uvádí minimální počet HDD. Řešení lze naplnit pomocí většího počtu menších HDD. Nikoliv však pomocí menšího počtu větších HDD. Požadavek je dán čistě s ohledem na výkon a dostupnost daného svazku.
- HW management serveru s možností zapnutí, vypnutí, restartu serveru, přesměrování KVM nezávisle na OS, vzdálené připojení médií, časově neomezená licence.
- Možnost rozšíření interního managementu o update serveru online (z OS) i bez nutnosti instalace dalšího nástroje pro správu, možnost bootu a instalace z interní SD karty.
- Podpora Silicon Root Of Trust, Secure Boot a Chain Of Trust (kontrola celého výrobního řetězce), TPM 2.0, RedFish API.

- Nejméně 2 za chodu vyměnitelné napájecí zdroje s platinovou účinností. Server musí být v dodávané konfiguraci schopen fungovat na jeden napájecí zdroj s tím, že jeho zátěž nesmí překročit 75%.
- Licence na Microsoft Windows Datacenter 2019 na všechna CPU jádra.
- Licence VMware vSphere Enterpise Plus na všechna CPU jádra.
- Dodavatel zajistí podporu výrobce 9x5 NBD v pracovních dnech se čtyřhodinovou reakční dobou v místě instalace, a to na dobu 5 let.

5. Fibre channel přepínače (volitelně)

- Montáž do standardního 19“ racku o maximální výšce 1 RU.
- Redundantní napájecí zdroje.
- Pokud to bloková disková pole vyžadují pro naplnění funkční specifikace je požadována dodávka FC přepínačů.
- Nejméně 24 aktivních portů.
- Certifikátem nebo čestným prohlášením potvrzená kompatibilita výrobce HBA serverů a zároveň diskových polí.
- Porty o rychlosti nejméně 32 Gbps.
- Licence na SW část zajišťující funkce, které Zadavatel požaduje aktivní. Jde o všechny běžné funkce FC přepínačů, zejména pak:
    - Hardwarově vynucený zóning
    - Filtrování rámců
    - In flight comprese a šifrování
    - Dynamické monitorování pro zajištění vysoké dostupnosti
    - Virtuální fabriky
    - ISL trunking
    - Integrované směrování
    - Management software, který umožní provádět konfigurace z webového prohlížeče, zónování, ladění, reporting událostí, zobrazení inventáře a telemetrických dat. Nástroj musí být on premise a musí být instalován na zálohovacím a management serveru. Systémové zdroje serveru musí být navýšeny o dvojnásobek doporučených systémových požadavků na výše uvedený software. Zejména pak CPU jádra, RAM, HDD-SSD, NIC a HBA.
- Podpora výrobce 24x7 non stop s 15ti minutovou reakční dobou výrobce vzdáleně a doručením náhradního dílu následujícího pracovního dne v místě instalace na 5 let.

6. Příslušenství pro datacenterové technologie

- Pro všechna zařízení datového centra zajistí Dodavatel následující: pro každý SFP+/SFP28/SFP56/QSFP28 či FC HBA patřičný multimode transceiver a patch kabel. Patch kabely budou vždy vedeny nad anebo pod rozvaděči. Odhadovaná potřebná délka patch kabelů je 5 metrů. Pro všechny FC technologie se z důvodu kompatibility nepřipouští použití OEM Transceiverů. Všechny FC technologie musí být prokazatelně vzájemně kompatibilní (uvedeno na oficiálních kompatibility listech výrobců).
- Pokud není k dispozici kabelový žlab, je nutné, aby si jej Dodavatel pro účel propojení racků a technologií dodělal. Tuto skutečnost si dodavatel případně může ověřit při prohlídce místa plnění.

- Racky jsou v různém technickém stavu a je nutné počítat s omezeným prostorem a omezenou nosností racků. Hloubka serverových racků je vždy nejméně 1200 mm. Zadavatel se nebrání dodávce nových racků Dodavatelem. V případě dodávky nového racku je na Dodavateli zajištění kabeláže do úrovně nadřazeného elektrického rozvaděče. Elektrická kabeláž musí zahrnout také ochranné lišty a požární ucpávky.
- Součástí dodávky musí být také patřičné napájecí kabely.
- Součástí každého zařízení musí být ližiny pro montáž do 19“ racku. Pokud to obsluha zařízení vyžaduje, musí být ližiny vysouvací.

7. Licence na zálohovací software

- Zálohovací software musí pracovat s infrastrukturou VMware založenou na verzích 6.0, 6.5 a 6.7, 7.0U3.
- Software musí podporovat hostitele spravované serverem VMware vCenter Server a samostatné hostitele.
- Software musí podporovat zálohování sdílených souborů ze zařízení založených na NAS pomocí sdílených složek SMB a NFS a přímo ze souborových serverů Windows a Linux.
- Software musí být možné licencovat v režimu instancí (bodů). Instance je možné použít na různé workloady (on-premise, cloud, fyzické servery, enterprise aplikace…) a různé programové balíčky výrobce. Software musí být nezávislý na hardware a musí využívat jakýkoli hardware serveru a úložiště.
- Software musí vytvářet samostatné zálohovací archivy ve formě souborů, které jsou volně přenositelné, s možností vytvářet takové soubory na úrovni zálohovací úlohy nebo na VM.
- Software musí umožňovat vytváření záloh v plném, syntetickém úplném, přírůstkovém a zpětném přírůstkovém režimu.
- Software musí mít mechanismy deduplikace a komprese, které vedou ke snížení objemu úložného prostoru pro zálohy. Povolení deduplikace a komprese nesmí omezit žádné funkcionality uvedené ve specifikaci.
- Software musí mít integraci se stávajícími diskovými poli HPE 3PAR v podobě podpory orchestrace vytváření aplikačně konzistentních snapshotů a to i logické disky, které jsou replikované na úrovni diskového pole.
- Software nesmí použít centrální databázi pro ukládání jakýchkoli metadat deduplikace. Ztráta databáze nemůže způsobit, že záložní soubory budou nestabilní. Metadata deduplikace musí být uložena v záložních souborech. Software nesmí vyžadovat instalaci jakéhokoli druhu stálého agenta uvnitř virtuálních počítačů, který vyžaduje údržbu, nasazení, upgrade atd. pro všechny operace zálohování a obnovy.
- Software musí nabízet samoobslužný portál, prostřednictvím kterého si uživatelé mohou obnovit soubory, virtuální počítače, objekty MS Exchange a databáze MS SQL, databáze Oracle (včetně obnovení v čase).
- Software musí být schopen integrace s jinými systémy pomocí zabudovaného rozhraní REST API zejména pak s nabízeným úložištěm pro nestrukturovaná data.
- Software musí nabízet šifrování celého síťového provozu mezi všemi komponentami a také šifrování "na cíli" záložních souborů v úložišti. Šifrování nemůže omezit žádné funkce uvedené ve specifikaci.
- Software musí využívat mechanismus sledování změn bloku. Pro všechny podporované hypervizory musí být implementace CBT certifikována výrobcem hypervizoru.

- Software musí být schopen kopírovat body obnovení a replikovat virtuální počítače do vzdáleného umístění pomocí technologie založené na vestavěné akceleraci WAN.
- Software musí mít replikaci produkčních VM přímo z infrastruktury VMware vSphere, mezi hostiteli ESXi, včetně asynchronní nepřetržité replikace. Software musí navíc umožnit jako zdroj replikačních úloh využít soubory záloh.
- Software musí umožňovat okamžitou obnovu více virtuálních strojů současně, přímo ze záložních souborů z libovolného bodu obnovení (externí NFS server). Tato funkce musí být podporována pro prostředí VMware a musí fungovat bez ohledu na hardware používaný k ukládání záložních souborů VM. Software musí umožňovat okamžitou obnovu prostředí ze zálohy NAS pomocí protokolu CIFS/SMB.
- Software musí umožňovat vytváření virtuální laboratoře (izolovaného prostředí) pro infrastrukturu VMware pomocí VM spuštěných přímo ze záložních souborů. Pro VMware musí nabídnout vytvoření takového prostředí přímo ze snímků úložiště vytvořených na podporovaných zařízeních.
- Software musí mít mechanismy ověřování obnovení zálohy umožňující testování obnovy virtuálních počítačů v izolovaném síťovém prostředí na infrastruktuře VMware. Ověření musí umožňovat testování aplikace uvnitř VM pomocí vlastních nebo předdefinovaných skriptů. Ověření musí být plánovatelné a zcela automatizované.

8. Pásková knihovna

- Knihovna bude osazena nejméně dvěma mechanikami LTO-8 s použitím protokolu FC. Je požadována technologie právě LTO-8, kvůli zajištění zpětné kompatibility s páskami LTO-7 a LTO7M.
- Pásková knihovna bude modulární a bude umožňovat rozšíření na nejméně 6 páskových mechanik. Bez rozšíření modulů bude knihovna schopna provozovat nejméně tři mechaniky.
- Montáž do standardního 19“ racku o maximální výšce 6 RU. A to i v případě rozšíření na 6 páskových mechanik.
- Redundantní napájecí zdroje.
- Podpora šifrování páskových médií.
- Buffer o velikosti nejméně 1GB. Minimální velikost bufferu je požadavek dán potřebou sekventizace provozu pro pásková média.
- Nejméně 40 pozic pro pásková média. Součástí dodávky bude 40 LTO-8 médií a jedno čistící médium. Počet pozice je dán požadavkem na kapacitu a operační komfort operátorů pro práci s médii.
- Podpora výrobce 9x5 NBD v pracovních dnech se čtyřhodinovou reakční dobou v místě instalace na 5 let.

9. Licence pro MS Windows server 2022 CAL

Operační systémy a jejich licence musí být plně kompatibilní se stávajícím prostředím Microsoft.

- Licence pro současně nejméně 1 Microsoft Windows Server 2022 CAL uživatelských licencí.

10. Licence pro další VMware technologie

Virtualizační farma musí být plně kompatibilní se stávajícím prostředím VMware.

- Licence pro vCenter Standard.

11. Licence pro VDI Technologii

VDI farma musí být plně kompatibilní se stávajícím prostředím VMware. Zadavatel připouští alternativní řešení. V takovém případě je nutné dodat kompletní řešení (virtualizace, management, monitoring a VDI) a je nutné zajistit úplnou kompatibilitu s instalovanými systémy. Následně Dodavatel zajistí zaškolení technických správců Zadavatele na odpovídající technickou úroveň tak, aby techničtí správci Zadavatele byli schopni poskytnout odpovídající servisní podporu uživatelům této technologie v nemocnici – náklady na dané zaškolení musí být obsahem nabídky dodavatele.

- V rámci implementace VDI technologií je potřeba zajistit dodávku následujících licencí: VMware Horizon 8 Enterprise pro 1 současně přihlášených uživatelů.
  Licence musí obsahovat následující funkce: Horizon View Manager, Workspace ONE Access Standard Edition, Application Remoting, Horizon for Linux, ThinApp, App Volumes, Dynamic Environment Manager Enterprise Edition, vSphere Desktop, and vCenter Server Desktop.Bez licencí vSAN, vRealize Operations pro Horizon a Fusion.

12. Souhrnné požadavky na datové přepínače

Souhrnné specifikaci musí vyhovět všechny modely dodávaných přepínačů (přístupové, páteřní, páteřní serverové), pokud není uvedeno jinak.

Bezpečnost

Jedním ze základních požadavků na datovou síť je zabezpečení přístupu k síťovým službám pouze pro oprávněné a pouze v nezbytně nutném rozsahu. Pro tento účel je požadováno, aby přístupové přepínače implementovaly řízení přístupu k síti dle modelu AAA s využitím protokolů IEEE 802.1X a RadSec a zabezpečený přístup k management rozhraní přepínačů protokolem TACACS+.

Pro zajištění maximální ochrany autentizačních dat při ověřování připojovaného klienta je požadováno šifrování komunikace mezi autentizátorem a autentizačním serverem s využitím protokolu RadSec. Aby byly dodrženy obecné zásady PKI na délku platnosti certifikátů a zároveň nevzrostla časová náročnost správy musí dodávané přepínače podporovat automatickou a bezpečnou distribuci certifikátů protokoly EST nebo SCEP. Zároveň dle doporučení Minimální požadavky na kryptografické algoritmy vydané Národním úřadem pro kybernetickou bezpečnost dne 8. 6. 2022 požaduje Zadavatel podporu RSA privátních klíčů délky 3072 bitů a delších. Za účelem včasné detekce nedostupnosti autentizačního serveru v časových intervalech, kdy nedochází k regulérnímu ověřování koncových klientů, musí přepínače podporovat aktivní monitorování dostupnosti RADIUS a TACACS+ serverů pomocí přednastaveného uživatelského jména a hesla.

Nezbytnou podmínkou pro bezpečnou datovou síť je zajištění integrity řetězce hardware – software přepínače proti neoprávněné modifikaci a to například ověřením podpisu obrazu operačního systému a použitím bezpečného zavaděče OS. Dalším požadavkem je konfigurovatelná ochrana control plane přepínače před DoS útoky cílenými na CPU přepínače.

Dodávané přepínače musí implementovat také obrané mechanizmy na úrovni vrstev L3 a L4 ISO modelu a to ochranu ARP protokolu (Dynamic ARP Protection), DHCP snooping, IP source guard a obdobné varianty pro protokol IPv6 (RA Guard, DHCPv6 Guard, IPv6 Destination Guard).

Pro směrování multicastového provozu je požadována podpora PIM-DM, PIM-SM, IPv6 PIM-SM, PIM-SSM a IPv6 PIM-SSM dále také podpora IGMP verze 2 a 3 a IGMP snooping.

Správa

U všech typů přístupových přepínačů je požadována dostupná sériová konzole pro zpřístupnění konfiguračního příkazového rozhraní. Přepínač musí podporovat příkazové rozhraní a uložené konfigurační soubory v textové formě čitelné člověkem. Funkčně neomezená správa přepínače musí být možná i bez přístupu do internetu. Pro striktní oddělení řídicí sítě od uživatelských dat je požadováno, aby přepínače měly dostupný Ethernetový tzv. Out-of-Band management port pro IP komunikaci s přepínačem. Dodávané přepínače musí umožnit rychlou obnovu konfigurace a instalaci firmware v off-line režimu prostřednictvím USB portu min. specifikace 2.0, ke kterému bude připojeno USB datové úložiště.

Vzdálená správa přepínačů bude probíhat autentizovanými a šifrovanými protokoly, je požadována implementace SNMPv3 klienta, SSHv2 serveru, HTTPS serveru. Pro souborový přenos musí přepínače implementovat SFTP a/nebo SCP klienta. Výše zmíněné protokoly musí být implementovány jak pro verzi IPv4, tak IPv6. S ohledem na rozsah datové sítě a omezené lidské zdroje IT oddělení Zadavatele je požadováno, aby pro automatizaci správy sítě byla na přepínačích dostupná aplikační rozhraní REST (včetně možnosti volání příkazů CLI rozhraní).

Pro zachování jednotné správy datové sítě Zadavatel požaduje, aby všechny přepínače využívaly stejný operační systém a jejich konfigurace byla prováděna stejně – konfigurační rozhraní přepínačů musí být identická. Je nezbytné, aby napříč přístupovými přepínači byly dostupné identické funkce a možnosti nastavení s přihlédnutím k rozdílům daným jiným počtem portů, NIC modulů a případnou dostupností napájení PoE.

S ohledem na umístění přepínačů v pobočkách Zadavatele, kde není lokálně zastoupena IT podpora je požadována možnost zachytávání síťové komunikace přímo na přepínačích se zápisem do souboru uloženém v lokálním úložišti přepínače. Takto uložená data ve formátu PCAP budou pak stažena pracovníkem IT oddělení a podrobena analýze nástrojem typu Wireshark. Pro účely bezpečnostní analýzy je požadováno zachycení provozu uplink portů v delších časových intervalech bez možnosti filtrování specifických toků ve velikosti minimálně 8 GB. Analýzu specifických toků, které lze identifikovat na základě fyzických portů a hlaviček protokolů vrstev L2 až L4 musí být možno provádět vzdáleně a to odesíláním zachytávaných paketů do vzdáleného analyzátoru typu WireShark (ERSPAN). Je nezbytné, aby přepínač podporoval alespoň čtyři obousměrná ERSPAN sezení. Dlouhodobá analýza síťového provozu bude prováděna pomocí sběru sFlow statistických dat síťových toků na přepínačích a jejich odesílání do sFlow kolektoru. Dodávané přepínače musí umožnit obousměrný (ingress a egress) sběr sFlow dle RFC 3176.

Pro zajištění vysoké kvality síťových služeb a jejich garanci Zadavatel požaduje dodání přepínačů s podporou techniky IP Service Level Agreement, které budou vystupovat v roli sondy (probe) i odpovídače (responder). S ohledem na využívané aplikace v rámci infrastruktury Zadavatele je požadována dostupnost SLA testů ICMP echo, UDP jitter, a TCP connect.

13. Přístupové přepínače

Zadavatel požaduje dodání nových přístupových přepínačů datové sítě, které splňují vysoké nároky na zabezpečení přístupu k síti, šifrování řídicích protokolů a kybernetickou bezpečnost samotných přepínačů.

Charakteristika přepínačů

V rámci topologického uspořádání datové sítě Zadavatele je požadováno dodání Ethernetových přepínačů s funkcí směrování IP provozu.

Fyzická instalace

Zařízení budou instalována do stávajících datových rozvaděčů a požaduje se dodání pouze takových přepínačů, které lze zamontovat do EIA rozvaděčů šířky 19 palců bez použití dodatečných polic. U všech typů přístupových přepínačů je požadována maximální výška 1RU. S ohledem na omezený prostor pro umístění rozvaděčů, často s možností pouze čelního přístupu, je nezbytné, aby byl přístup k datovým portům a ovládacím prvků z čelní strany rozvaděče. Umístění datových portů ze zadní strany se připouští pouze pro stohovací propojení, přičemž musí být zajištěna ochrana proti zlomení zejména optických kabelů.

Dodávané přepínače musí být možno zamontovat vodorovně do rozvaděče o šířce 600 mm a hloubce 395 mm a musí být umožněno uzavření a uzamčení dveří rozvaděče. Připouští se, aby dodavatel vyměnil rozvaděč za hlubší. V tomto případě musí dodavatel přesunout veškeré stávající vybavení do nového rozvaděče, ve kterém musí být instalovány a použity organizéry pro datové a napájecí kabely včetně horizontálních vyvazovacích panelů. Dodavatel je také povinen zajistit případné elektrické práce při případném přesunu el. zásuvek a doložit revizní zprávy k provedeným změnám.

Výjimku tvoří malé přepínače, které jsou umístěny na vodorovném povrchu v kancelářských prostorech (položeny na kancelářském stole). U těchto přepínačů je požadován provoz bez aktivního chlazení ventilátorem.

Všechny typu přepínačů musí být možné provozovat v prostředí s okolní teplotou 45 °C. Většina rozvaděčů není umístěna v klimatizovaných místnostech a chlazení vnitřního prostoru rozvaděče probíhá pouze prouděním okolního vzduchu větracími otvory rozvaděče.

Specifikace portů

Zadavatel požaduje dodání následujících typů přístupových přepínačů.

- přepínače se 48 přístupovými porty typu 1000BASE-T, minimálně 2 porty SFP+ o kapacitě 10 Gbps, minimální požadovaný přepínací výkon 136 Gbps, paketový výkon 127 Mpps;
- přepínače s 24 přístupovými porty typu 1000BASE-T, minimálně 2 porty SFP+ o kapacitě 10 Gbps, minimální požadovaný přepínací výkon 88 Gbps, paketový výkon 65 Mpps;
- přepínače s 12 přístupovými porty typu 1000BASE-T, minimálně 2 porty SFP+ o kapacitě 10 Gbps, minimální požadovaný přepínací výkon 64 Gbps, paketový výkon 47 Mpps.

Všechny přístupové porty musí podporovat přenosové rychlosti 10/100/1000 Mbps v poloviční i plném duplexu.

Pro všechny typy přístupových přepínačů je požadováno, aby všechny přístupové porty podporovaly napájení koncových zařízení dle standardu IEEE 802.3at (Class 4). Pro minimalizování doby výpadku služeb využívajících zařízení napájených prostřednictvím přístupových přepínačů, jako jsou například IP telefony a bezdrátové přístupové body, musí přepínače podporovat trvalé doručování napájení PoE i v případě restartování přepínače a také umožnit rychlé zapnutí PoE napájení pro koncová zařízení ihned po připojení napájení ke zdroji přepínače bez čekání na naběhnutí operačního systému. Přístupové porty všech typů přepínačů musí podporovat standard IEEE 802.3az.

U všech výše uvedených typů přepínačů požadujeme nejméně dva *uplink* porty typu SFP+ pro připojení do datové sítě. Z důvodu různých typů, kvality a délek stávající strukturované optické a metalické kabeláže musí tyto porty podporovat použití vložných modulů 1000BASE-SX, 1000BASE-LX, 1000BASE-T, 10GBASE-SR, 10GBASE-LR a 10GBASE-T.

Podpora stohování

Topologie datové sítě počítá s agregací přepínačů v jednotlivých podružných rozvaděčích do tzv. stohů s cílem zajistit vysokou dostupnost datové sítě a zjednodušit její správu. Stohování je požadováno s ohledem na omezený počet dostupných optických a metalických spojů vedoucích do podružných rozvaděčů a je požadováno pro všechny typy přístupových přepínačů.

Počet přepínačů, které lze sloučit do jednoho stohu, musí být minimálně šest a je požadována možnost spojovat mezi sebou přepínače různých typů (s napájením i bez napájení PoE, o kapacitě 24 i 48 přístupových portů). Z důvodu redundance musí být v rámci stohu nejméně dva přepínače v roli řídicích prvků, jeden aktivní a druhý záložní. V případě výpadku aktivního řídicího přepínače je okamžitě aktivován záložní přepínač a nesmí dojít k rozpadnutí stohu ani vynuceného restartu žádného z dalších přepínačů. Je nezbytné, aby přepínače ve stohu byly propojeny redundantně – výpadek jedno stohovacího spoje nebo jednoho přepínače nesmí způsobit tzv. split brain. Po propojení stohovacích linek 24 a 48 portových přepínačů musí na každém přepínači zůstat minimálně dva volné SFP+ uplink porty, každý o dostupné kapacitě 10 Gbps. Aby bylo zajištěno spolehlivé fungování stohu z pohledu přepínání rámců, je nutné, aby byla podporována propustnost stohování pro 12 portové přepínače nejméně 20 Gbps obousměrně, pro 24 portové přepínače nejméně 40 Gbps obousměrně a pro 48 portové přepínače nejméně 80 Gbps obousměrně. S ohledem na dostupnost linek strukturované kabeláže Zadavatel požaduje, aby přepínače tvořící jeden stoh mohly být umístěny v oddělených datových rozvaděčích, které jsou od sebe vzdáleny 10 metrů.

Výsledný stoh musí vystupovat jako jeden technologický přepínač a tedy být konfigurovatelný pomocí jedné management IP adresy, mít jeden konfigurační soubor a chovat se jako jedno L3 zařízení včetně podpory dynamických směrovacích protokolů jako je OSPF. Stoh tedy musí umožnit i konfiguraci portů z různých členů do jedné IEEE 802.1AX agregace Ethernetových linek řízené protokolem LACP.

Funkce přepínače

Zadavatel požaduje dodání přepínačů s podporou tzv. jumbo rámců o minimální velikosti 9000 B. Pro snížení dopadu při přepínání nárazových shluků rámců s ohledem na připojení bezdrátových AP je na přepínačích požadována minimální velikost paketové vyrovnávací paměti 8 MB. Minimální požadovaný počet záznamů v tabulce MAC adres je 32000.

Pro zajištění síťové topologie bez technologických smyček musí přepínače podporovat protokol MSTP dle IEEE 802.1s a také Rapid Spanning Tree dle IEEE 802.1w. Pro správné ošetření stavů, kdy dojde vlivem poškození kabeláže nebo portu přepínače k jednosměrné komunikaci musí přepínače implementovat funkcionalitu UDLD (Unidirectional Link Detection) nebo odpovídající. Za účelem zvýšení ochrany sítě musí přepínače na jednotlivých portech podporovat ochranu zahlcení a to omezením na úrovni počtu přepínaných rámců a bitů za vteřinu. Dodávané přepínače musí podporovat tunelování rámců Q-in-Q dle IEEE 802.1ad a je požadována i možnost překladu identifikátoru VLAN v 802.1Q značkách. Pro snížení konfigurační složitosti při vytváření a mazání VLAN v rámci datové sítě a optimalizované šíření broadcast a multicast provozu je požadována implementace protokolu MVRP. S ohledem na připojování speciálních nemocničních zařízení, která mají nedostatečné možnosti zabezpečení síťového rozhraní, je požadováno, aby přepínače podporovaly nastavení izolovaných L2 segmentů sítě, tzv. privátních VLAN, ve kterých je blokována vzájemná komunikace připojených klientů mezi sebou. V rámci těchto segmentů je požadována tvorba podřízených segmentů, kde bude umožněna komunikace klientů mezi sebou – tzv. komunitní segmenty (community VLAN). Jedná se například o připojení ovládacích panelů k diagnostickým zařízením.

Přístupové přepínače musí implementovat protokol LLDP a LLDP-MED, který je nezbytný pro automatické nastavení parametrů VoIP telefonů (VLAN ID, priorita provozu) a pro vyjednání napájení prostřednictvím PoE.

Zadavatel hodlá využívat agregování Ethernetových linek, aby byl maximálně využit potenciál dostupné strukturované kabeláže a zajištěna vysoká dostupnost spojení. Pro tyto účely musí přepínače podporovat dynamicky řízenou agregaci protokolem LACP, kde každý přepínač musí podporovat minimálně 20 agregačních skupin a skupinu o minimálně 8 portech. Zároveň je vyžadována možnost konfigurace rozkládání zátěže mezi jednotlivé porty agregační skupiny a to na základě hlaviček protokolů L2, L3 a L4 vrstev modelu ISO.

Bezpečnost

S přihlédnutím k typům zařízení, která jsou připojena do datové sítě Zadavatele, je nutné, aby dodávané přepínače podporovaly ověření dle 802.1X a RFC 4675 a minimálně 8 klientů připojených za jedním fyzickým portem a dále tzv. MAC bypass autentizaci. Datová síť připojuje i IP telefony, jejichž funkčnost je kritická z pohledu hlášení a řešení krizových situací například v případě požáru. Pro zajištění síťové dostupnosti pro tyto systémy je požadováno, aby v případě nedostupnosti autentizačního serveru přepínače umožnily konfiguraci tzv. Critical Voice VLAN. Pro ostatní systémy je pro případ nedostupnosti autentizačního serveru požadována konfigurační možnost přidělení alespoň omezeného přístupu do sítě přiřazením do tzv. Critical VLAN. Pro autentizaci a autorizaci rozdílných připojovaných klientů je na přepínačích vyžadována možnost nastavení různé kombinace a pořadí metod ověření (IEEE 802.1X, MAC bypass, trvale autentizované). Zadavatel požaduje, aby výsledkem autentizačního procesu bylo kromě přiřazení klienta do správného L2 segmentu sítě a nastavení priority provozu také nastavení komplexní uživatelské role, která definuje povolené VLANy v případě trunkového portu pro připojení AP, nastavení DSCP značkování klientského provozu, filtrování paketů dle ACL, nastavení omezení šířky přenosového pásma. V rámci nastavení QoS musí přepínače implementovat minimálně osm prioritních paketových front. Aby bylo možno spravovat omezení přístupu autentizovaných klientů na základě přiřazených ACL z centrálního autentizačního serveru je požadováno, aby přepínače pro tento účel podporovaly RADIUS atribut NAS-Filter-Rule dle RFC 4849. Připouští se výrobcem implementované vlastní řešení transportu uživatelských rolí, které bude kryptograficky zabezpečeno například využitím SSL. Přepínače musí umožnit lokální definici těchto rolí v konfiguračním souboru, tyto role se využijí v případě nedostupnosti autentizačního serveru.

Správa

Zadavatele požaduje, aby přepínače na přístupových portech podporovaly vzdálenou diagnostiku kabeláže, metodou Time Domain Reflectometry nebo obdobnou. V případě použití jiné techniky ověří Dodavatel se Zadavatelem akceptovatelnost obdobnosti objektivním způsobem.

14. Páteřní a páteřní serverové přepínače

Zadavatel požaduje dodání výkonných a spolehlivých přepínačů, které budou agregovat optické uplink spoje přístupových přepínačů, připojovat serverovou infrastrukturu a tvořit páteřní část datové sítě.

Fyzická instalace

Zařízení budou instalována do stávajících datových rozvaděčů a požaduje se dodání pouze takových přepínačů, které lze zamontovat do EIA rozvaděčů šířky 19 palců bez použití dodatečných polic. U všech typů páteřních přepínačů je požadována maximální výška 1RU. Dodávané přepínače

musí být možno zamontovat vodorovně do rozvaděče o šířce 600 mm a hloubce 800 mm a musí být umožněno uzavření a uzamčení dveří rozvaděče.

Dodávané přepínače musí mít zajištěnu redundanci interních napájecích zdrojů vyměnitelných za běhu a redundanci ventilátorů vyměnitelných za běhu. Přepínač musí být schopen bez výpadku pokračovat v provozu při poruše jednoho ventilátoru nebo jednoho napájecího zdroje.

Specifikace portů páteřních přepínačů

Zadavatel požaduje dodání následujícího typu páteřního přepínače.

- Přepínač se 48 SFP+ přístupovými porty a minimálně 2 uplink porty o minimální rychlosti 40 Gbps, minimální požadovaný přepínací výkon 1120 Gbps, paketový výkon 1600 Mpps.

Výše specifikované přístupové porty musí podporovat přenosové rychlosti 1/10 Gbps. Z důvodu různých typů, kvality a délek stávající strukturované optické a metalické kabeláže musí tyto porty podporovat použití vložných modulů 1000BASE-SX, 1000BASE-LX, 1000BASE-T, 10GBASE-SR, 10GBASE-LR a 10GBASE-T. Uplink porty musí podporovat vložné moduly, které umožní propojení s páteřními přepínači pomocí tzv. single-mode optických kabelů třídy OS-2 na vzdálenost delší než 500 m.

Specifikace portů páteřních serverových přepínačů

Zadavatel požaduje dodání následujících typů páteřních serverových přepínačů.

- Pro velkou lokalitu přepínače se 48 přístupovými SFP28 porty a minimálně 2 uplink porty o minimální rychlosti 40 Gbps pro připojení páteřního přepínače a minimálně 2 uplink porty o minimální rychlosti 100 Gbps pro připojení druhé velké lokality, minimální požadovaný přepínací výkon 2960 Gbps, paketový výkon 2200 Mpps.
- Pro malou lokalitu přepínače s 24 přístupovými SFP+ porty a minimálně 2 uplink porty o minimální rychlosti 25 Gbps pro připojení do velké lokality, minimální požadovaný přepínací výkon 580 Gbps, paketový výkon 432 Mpps.

Přístupové porty přepínače velké lokality musí podporovat přenosové rychlosti 1/10/25 Gbps a použití vložných modulů 1000BASE-SX, 1000BASE-LX, 1000BASE-T, 10GBASE-SR, 10GBASE-LR, 10GBASE-T, 25GBASE-SR a 25GBASE-LR. Přístupové porty přepínače malé lokality musí podporovat přenosové rychlosti 1/10 Gbps a použití vložných modulů 1000BASE-SX, 1000BASE-LX, 1000BASE-T, 10GBASE-SR, 10GBASE-LR, 10GBASE-T.

Podpora stohování

Zadavatel počítá s agregací přepínačů do tzv. stohů s cílem zajistit vysokou dostupnost datové sítě a zjednodušit její správu. Počet přepínačů, které lze sloučit do jednoho stohu, musí být minimálně dva. Z důvodu redundance musí být v rámci stohu nejméně dva přepínače v roli řídicích prvků. V případě výpadku jednoho řídicího přepínače nesmí dojít k rozpadnutí stohu ani vynucenému restartu žádného z dalších přepínačů. Je nezbytné, aby přepínače ve stohu byly propojeny redundantně – výpadek jedno stohovacího spoje nebo jednoho přepínače nesmí způsobit tzv. split brain. Aby bylo zajištěno spolehlivé fungování stohu z pohledu přepínání rámců je nutné, aby byla podporována propustnost stohování nejméně 200 Gbps obousměrně pro páteřní přepínače, pro páteřní serverové přepínače malé lokality nejméně 200 Gbps obousměrně a pro páteřní serverové přepínače velké lokality nejméně 400 Gbps obousměrně. V rámci stohu musí být podporováno distribuované přepínání paketů a je požadováno, aby přepínače tvořící jeden stoh mohly být umístěny v oddělených datových rozvaděčích v rozdílných místnostech, které jsou od sebe vzdáleny 100 a více metrů.

Po redundantním propojení přepínačů do jednoho stohu musí na každém přepínači zůstat výše definované minimální počty uplink portů.

Funkce páteřního přepínače

Zadavatel požaduje dodání přepínačů s podporou tzv. jumbo rámců o minimální velikosti 9000 B. Pro vyrovnávání nárazových shluků rámců je na přepínačích požadována minimální velikost paketové vyrovnávací paměti 16 MB. Pro vyloučení přetížení ve směru incast a pro vyloučení přetížení ASICů je požadovaná minimální vyrovnávací paměť. Tato funkce je kritická pro neblokující architekturu přepínačů. Minimální požadovaný počet záznamů v tabulce MAC adres je 64000. Přepínače musí implementovat protokol LLDP a LLDP-MED.

Pro zajištění síťové topologie bez logických smyček musí přepínače implementovat protokol MSTP dle IEEE 802.1s a Rapid Spanning Tree dle IEEE 802.1w Pro správné ošetření stavů, kdy dojde vlivem poškození kabeláže nebo portu přepínače k jednosměrné komunikaci musí přepínače implementovat funkcionalitu UDLD (Unidirectional Link Detection) nebo odpovídající. Za účelem zvýšení ochrany sítě musí přepínače na jednotlivých portech podporovat ochranu zahlcení a to omezením na úrovni počtu přepínaných rámců a bitů za vteřinu. Dodávané přepínače musí podporovat tunelování rámců Q-in-Q dle IEEE 802.1ad a je požadována i možnost překladu identifikátoru VLAN v 802.1Q značkách. Pro snížení konfigurační složitosti při vytváření a mazání VLAN v rámci datové sítě a optimalizované šíření broadcast a multicast provozu je požadována implementace protokolu MVRP. Je požadováno, aby přepínače podporovaly nastavení izolovaných L2 segmentů sítě, tzv. privátních VLAN, ve kterých je blokována vzájemná komunikace připojených klientů mezi sebou. V rámci těchto segmentů je požadována tvorba podřízených segmentů, kde bude umožněna komunikace klientů mezi sebou – tzv. komunitní segmenty (community VLAN).

V rámci nastavení QoS musí přepínače implementovat minimálně osm prioritních paketových front. Dále je požadována možnost nastavení důvěryhodnosti značkování příchozích rámců a možnost přeznačkování provozu klasifikovaného pomocí ACL.

Zadavatel hodlá využívat agregování Ethernetových linek, aby byl maximálně využit potenciál dostupné strukturované kabeláže a zajištěna vysoká dostupnost spojení. Pro tyto účely musí přepínače podporovat dynamicky řízenou agregaci protokolem LACP dle IEEE 802.1AX, kde každý přepínač musí podporovat minimálně 48 agregačních skupin a skupinu o minimálně 8 portech. Zároveň je vyžadována možnost konfigurace rozkládání zátěže mezi jednotlivé porty agregační skupiny na základě atributů L2, L3 a L4 vrstev modelu ISO.

Funkce páteřního serverového přepínače

Zadavatel požaduje dodání páteřních serverových přepínačů, které splňují minimálně stejné funkce, jako jsou uvedeny u páteřních přepínačů. Pro vyrovnávání nárazových shluků rámců je na přepínačích požadována minimální velikost paketové vyrovnávací paměti pro přepínače velkých lokalit 32 MB, pro malé lokality 16 MB. Pro vyloučení přetížení ve směru incast a pro vyloučení přetížení ASICů je požadovaná minimální vyrovnávací paměť. Tato funkce je kritická pro neblokující architekturu přepínačů. Minimální požadovaný počet záznamů v tabulce MAC adres je pro velké lokality 96000 a pro malé lokality 32000.

Požadovaná množina funkcí páteřních přepínačů je rozšířena o technologie směrování paketů. Přepínače určené pro velké lokality musí podporovat minimálně 96000 záznamů v tabulce ARP. Dále je požadována implementace DHCP serveru a relay pro IPv4 a IPv6 včetně podpory VRF. Pro zajištění redundance podpora protokolů VRRPv2 a VRRPv3.

Pro automatickou distribuci směrovacích informací musí přepínače podporovat dynamické směrovací protokoly OSPFv3 a BGP a to pro protokoly IPv4 a IPv6 včetně redistribuce a filtrování pomocí route map. Pro řešení výjimek směrování je požadována implementace tzv. policy based směrování. Při existenci více cest pro daný směrovací záznam musí přepínače podporovat funkci ECMP směrování včetně deterministického rozkládání zátěže.

Přepínače musí umožnit klasifikaci přepínaných rámců (ACL) na úrovni zdrojové a cílové MAC adresy, zdrojové a cílové IPv4 / IPv6 adresy, čísla zdrojového a cílového portu a protokolu.

Bezpečnost

S přihlédnutím k typům zařízení, která jsou připojena do datové sítě Zadavatele, je nutné, aby dodávané přepínače podporovaly ověření dle 802.1X a RFC 4675 a to včetně samostatného ověření minimálně 24 klientů připojených za jedním fyzickým portem a dále tzv. MAC bypass autentizaci. Pro případ nedostupnosti autentizačního serveru je požadována konfigurační možnost přidělení alespoň omezeného přístupu do sítě přiřazením do tzv. Critical VLAN. Pro autentizaci a autorizaci rozdílných připojovaných klientů je na přepínačích vyžadována možnost nastavení různé kombinace a pořadí metod ověření (IEEE 802.1X, MAC bypass, trvale autentizované).

Zadavatel uvažuje o vysokokapacitním propojení velkých lokalit pomocí optických spojů, které budou poskytovány třetí stranou. Za účelem zajištění integrity a důvěrnosti přenášených dat bude komunikace zabezpečena protokolem MACsec. Z tohoto důvodu Dodavatel požaduje, aby páteřní přepínače pro velké lokality podporovaly na 100 Gbps uplink portech šifrování provozu MACsec s využitím 256 bitového klíče AES.

15. Bezdrátový přístupový bod (Wi-Fi Access Point)

V rámci projektu obnovy síťové infrastruktury Zadavatel požaduje dodání bezdrátové počítačové sítě dle standardu 802.11. Tato bezdrátová síť bude primárně určena pro připojení klientů ve správě Zadavatele a to zejména pracovních počítačů zdravotnického personálu a ostatních zaměstnanců v nemocnici, medicínských přístrojů a dalších nemocničních zařízení, která pro svou činnost vyžadují připojení do počítačové sítě Zadavatele. Další službou bude poskytování bezdrátového připojení pacientů a návštěvníků nemocnice pro přístup do veřejného internetu.

Režim AP

Topologie datové sítě počítá s nasazením bezdrátových přístupových bodů centrálně řízených řadičem bezdrátové sítě a to zejména z důvodu jednoduché implementace a následné správy. AP musí být plně podporovány dodávaným řadičem bezdrátové sítě. Pro případ instalace ve vzdálených lokalitách, které běží v částečně izolovaném režimu je požadováno, aby AP mohlo být provozováno v autonomním režimu (bez kontroléru).

V případě mimořádné situace, kdy dojde ke ztrátě či znemožnění kabelového spojení mezi přístupovými přepínači, je záložním plánem pro rychlou obnovu datové komunikace použití bezdrátových přístupových bodů v režimu Wi-Fi Mesh. AP musí podporovat režim Wi-Fi Mesh včetně dynamického určení cesty k bodu, který je v roli brány a poskytuje připojení do datové sítě.

Pro zajištění služeb bezdrátové sítě je nutné, aby celý systém mohl být dlouhodobě provozován, a to včetně konfiguračních změn, bez přístupu do veřejného internetu. Tento krizový scénář může nastat např. při preventivním odpojení celé vnitřní sítě Zadavatele od veřejného internetu při reakci na kybernetický útok.

Fyzická instalace

Z důvodu instalace bezdrátových přístupových bodů (dále jen AP) v nemocničním prostředí jsou požadovány AP pro vnitřní instalaci uzavřené konstrukce bez větracích otvorů a bez aktivního chlazení, jejichž rozsah pracovních teplot okolního prostředí je od 0 °C do +50 °C. AP musí v tomto rozsahu pracovat bez omezení vysílacího výkonu a bez omezení funkcí. Většina prostorů, kde budou přístupové body instalovány, není klimatizována a nelze tak zaručit stabilní teplotní prostředí. Předpokládá se instalace AP v prostorách přístupných veřejnosti bez trvalého kamerového dohledu a proto je požadována možnost dodatečného fyzického zajištění pomocí slotu Kensington.

V případě instalace na pokojích na lůžkových odděleních je požadována možnost vypnutí indikačních LED diod na AP.

Omezený instalační prostor daný konstrukcí nemocničních budov vyžaduje použití AP s interními anténami. Předpokládá se montáž na strop a pro maximální pokrytí podlahové plochy jsou požadovány AP s všesměrovou vysílací charakteristikou skloněnou směrem k zemi (down-tilt). Součástí dodávky AP je příslušenství pro montáž na strop nebo na zeď.

Připojení do LAN

Zadavatel požaduje připojení AP do jednotné síťové infrastruktury, která bude tvořit transportní vrstvu pro řídicí signály mezi řadičem bezdrátové sítě a AP (tzv. control plane) a zároveň bude přenášet klientská data (data plane). Z důvodu zajištění vysoké dostupnosti jednotlivých AP je požadována redundance datového spojení do sítě LAN. AP musí disponovat minimálně dvěmi Ethernetovými porty, které umožňují sestavit dynamickou linkovou agregaci dle protokolu LACP. Zároveň je požadováno, aby oba porty umožňovaly napájení AP pomocí Power over Ethernet a to v režimu bezvýpadkového přepínání. Odpojení jednoho libovolného portu nesmí způsobit výpadek napájení a odpojení asociovaných klientů od AP. Pro minimalizaci dodatečných nákladů na instalaci a provoz bezdrátové sítě je požadováno napájení AP z přístupových přepínačů sítě LAN. Dodávané AP musí být provozuschopné při napájení jedním Ethernetovým portem dle specifikace IEEE 802.3at (Class 4) a to bez omezení vysílacího výkonu všech rádií. Pro případ instalace v prostorech, kde není dostupná nebo není možno instalovat datovou kabeláž, je požadována možnost napájení AP z externího AC adaptéru.

V rámci programu snižování energetické náročnosti Zadavatel požaduje, aby AP umožňovaly přechod do režimu hlubokého spánku, kdy jsou vypnuta všechna rádia a USB port. Zároveň musí být možné AP z tohoto režimu vzdáleně probudit bez nutnosti zasahovat do konfigurace přístupového přepínače. Jedná se o opatření použité v prostorách, kde bezdrátová síť nemusí být trvale dostupná (ordinace, kanceláře mimo pracovní dobu).

Rádiové rozhraní

S ohledem na vytížení frekvenčního pásma v rozsahu 2.4 GHz, které je sdíleno velkým množstvím technologií jiných než 802.11, je na AP požadována podpora i frekvenčních pásem 5 GHz a 6 GHz. Pro zajištění kompatibility se stávajícím bezdrátovými klienty musí AP podporovat standardy IEEE 802.11a/b/g/n, 802.11ac wave2 a 802.11ax. Dodaná AP musí být certifikována Wi-Fi Alliance a to Wi-Fi CERTIFIED a, b, g, n, ac a Wi-Fi CERTIFIED 6E (ax, 6 GHz). Dodávaná AP musí podporovat minimálně 4 SSID na každé rádio.

Minimální požadovaná konfigurace je 2x2:2 MIMO pro všechna frekvenční pásma (2.4 GHz, 5 GHz a 6 GHz). Zadavatel požaduje, aby AP podporovalo OFDMA multiplexování pro uplink i downlink. Pro optimalizaci dostupnosti bezdrátové konektivity pro mobilní klienty je požadováno, aby dodávaná

AP podporovala funkci Target Wait Time. V určitých místech instalace se předpokládá vyšší hustota AP a tedy větší pravděpodobnost překryvu vysílacích kanálů a je nutné, aby dodávaná technologie uměla BSS Coloring pro adaptivní řešení problémů s možným rušením 802.11 provozu. Ve zdravotnických zařízeních je typické shlukování klientů bezdrátové sítě v omezených prostorách jako jsou vstupní haly a čekárny, kdy typicky dochází k nerovnoměrnému rozdělení klientů mezi dostupné AP a ke značnému zhoršení kvality služby bezdrátové sítě kvůli vysokému vytížení jednotlivých AP. Dodávaná technologie musí umožnit dynamické vyvažování klientů mezi dostupná okolní AP s ohledem na aktuální zátěž, počet klientů a sílu signálu a to i pomocí asistovaného přesunu klienta do jiného frekvenčního pásma, tzv. Band Steering. Vzhledem k různorodosti implementace algoritmů výběru BSSID na straně klientů je požadována možnost konfigurace doporučeného i vynuceného přechodu do jiného frekvenčního pásma a podpora přesunu klienta na 802.11ax rádio.

Zadavatel plánuje obnovu bezdrátové sítě s předpokládaným využitím i pro kontrolní a řídicí prvky inteligentní budovy se zaměřením na zvýšení bezpečnosti a kvality provozu a snížení energetické náročnosti nemocničních budov. Je požadováno dodání AP, která mají integrované rádio Bluetooth verze 5.0 Low Energy a integrované rádio Zigbee IEEE 802.15.4.

Řízení provozu

Pro zajištění nepřetržité dostupnosti bezdrátové konektivity pro mobilní zařízení je ze strany bezdrátové sítě nutná podpora standardu IEEE 802.11r pro rychlou autentizaci klienta při přechodu mezi jednotlivými AP. V síti Zadavatele se nachází i starší bezdrátová zařízení, která nemají implementovánu podporu 802.11r, případně jejich ovladače bezdrátového rozhraní obsahují chyby v implementaci 802.11r. Pro tyto případy bude vytvořeno samostatné SSID a dodávané AP musí podporovat funkci Pairwise Master Key Caching dle IEEE 802.11i. Bezdrátová síť musí také podporovat distribuci PMK klíčů mezi připojenými AP tak, aby klient při přechodu mezi jednotlivými AP nemusel být ověřen protokolem EAP a došlo tak ke zkrácení procesu ověření. Požadavek je kladen zejména kvůli časové složitosti EAP autentizace, která je navíc značně ovlivněna implementací výše zmíněných starších zařízení.

Zajištění spolehlivé síťové komunikace pro kritické a důležité aplikace využívané Zadavatelem znamená garanci kvality služby datových přenosů přes sdílené komunikační médium. Přístupové body bezdrátové sítě musí umožňovat řízení kvality služby na základě rozpoznání aplikačních toků. IP pakety vybraných aplikací budou označeny DSCP značkou pro prioritizované řízení provozu v případě saturace komunikačního rozhraní. AP musí být schopno rozpoznávat kategorie aplikací na 7. vrstvě síťového modelu ISO případně pomocí signatur. Nestačí detekce pouze na základě hlaviček IP protokolu či transportních protokolů, protože by docházelo k hrubé a velmi nepřesné kategorizaci zejména cloudových aplikací běžících nad aplikačním protokolem HTTP.

Pro specifické účely nemocničních zařízení budou v bezdrátové síti Zadavatele vytvořeny lokálně platné a izolované SSID. AP musí umožnit přepínat klientský provoz z izolovaného SSID do specifického VLAN segmentu přímo na portu AP. Zároveň je nutné zajistit dynamickou adresaci připojených klientů protokolem DHCP. Je nezbytná podpora spuštění lokálního DHCP serveru na AP, který bude přiřazovat IP adresy klientům v izolovaných sítích.

Bezpečnost

Klíčovým požadavkem na bezdrátovou síť je zajištění maximální možné bezpečnosti přenášených dat a dostupnosti připojení. Vzhledem k povaze šíření rádiového signálu v prostoru, který

je v případě zdravotnických zařízení navíc veřejně přístupný, je nutné použít i opatření, která cílí na již probíhající pasivní a aktivní útoky na bezdrátovou síť.

Základní bezpečnostní rolí je umožnit komunikaci prostřednictvím bezdrátové datové sítě pouze autorizovaným uživatelům a zabezpečit jejich přenášená data proti odposlechnutí a podvržení. Pro dosažení tohoto cíle musí být dodávaná AP certifikována Wi-Fi aliancí dle specifikace WPA3-Enterprise a WPA3-Personal. AP musí podporovat symetrické šifrování přenášených dat pomocí 192 bitové klíče a použití šifrovacího algoritmu z rodiny CNSA. Pro ověřování klientů při přístupu do návštěvnické sítě je vyžadována implementace WPA3-OWE. Vzhledem k otevřenosti návštěvnické sítě a žádné kontroly nad připojovanými zařízeními je vyžadována možnost izolace bezdrátových klientů na 2. vrstvě síťového modelu ISO pro specifické SSID.

Pro bezpečné řízení klientů bezdrátové sítě je požadována implementace ochrany 802.11 management rámců dle standardu IEEE 802.11w.

Pro zajištění maximální ochrany autentizačních dat při ověřování připojovaného klienta je požadováno šifrování komunikace mezi AP a autentizačním serverem s využitím standardního protokolu RadSec. AP vystupuje v roli komunikační brány pro bezdrátové klienty pro přístup do datové sítě Zadavatele. Z pohledu datové sítě je takový přístup možný pouze tehdy, pokud dojde k ověření identity a autorizaci klienta a to platí i pro mezičlánek, kterým je AP. Proto je požadováno, aby AP podporovalo ověření na LAN portech v roli klienta (supplicant) a to v režimu vzájemného ověření s autentizačním serverem metodami PEAP a EAP-TLS. S ohledem na možnost fyzického přístupu neoprávněných osob k AP je nutné, aby byla vhodným způsobem zabezpečena důvěryhodnost řetězce hardware – software AP proti neoprávněné modifikaci a to například ověřením podpisu obrazu operačního systému a použitím bezpečného zavaděče OS.

Nedílnou součástí zabezpečení bezdrátové sítě je detekce útoků a hrozeb na úrovni 802.11 komunikace tzv. Wireless Intrusion Detection. Po dodávaném řešení se požaduje, aby současně s obsluhou legitimních bezdrátových klientů probíhalo kontinuální bezpečnostní skenování a kontinuální spektrální analýza pásem bezdrátové sítě. Takto získaná data budou korelována s výstupy z ostatních AP a vyhodnocena za účelem detekce škodlivých AP, útoků typu Man-in-The-Middle, podvržení MAC adres, HoneypotAP a dalších hrozeb a pro vyhodnocení elektromagnetického rušení nepocházejícího z 802.11 komunikace.

Bezdrátová síť musí být schopna prostřednictvím AP aktivní obrany proti škodlivým stanicím a klientům. Dodávaná AP proto musí podporovat techniky zamezení přístupu klientů ke škodlivým AP pomocí opakovaného zasílání deautentizačních rámců. Pro případy, kdy tato metodika není dostatečně účinná, např. při nasazení ochrany řídicích rámců, musí AP podporovat metodu ochrany pomocí vynucené asociace s falešným BSSID nebo použitím falešného kanálu.

Údržba

AP musí být vybaveno USB portem v minimální specifikaci 2.0. Pro servisní účely musí být AP vybaveno sériovým konzolovým portem, který zpřístupní příkazové konfigurační rozhraní.

S ohledem na umístění AP v pobočkách Zadavatele, kde není lokálně zastoupena IT podpora a pro maximálně efektivní využití omezených lidských zdrojů IT oddělení Zadavatele je požadováno, aby řešení problémů s provozem bezdrátové sítě mohlo být prováděno vzdáleně bez nutnosti zásahu v místě instalace AP. Z tohoto důvodu je požadována možnost zachytávání bezdrátových rámců,

včetně 802.11 hlaviček, přímo samotným AP a zasílání těchto dat ve standardním formátu PCAP do Ethernetového analyzátoru.

Pro možnost vzdálené instalace AP, kdy montáž není prováděna IT pracovníkem, je nezbytné aby AP podporovalo tzv. Zero Touch Provisioning, který umožní zcela automatickou prvotní konfiguraci AP s využitím externího management nástroje tak, aby se AP připojilo k řadiči bezdrátové sítě bez nutnosti jakékoliv konfigurační přípravy na straně infrastruktury Zadavatele.

Pro vzdálenou správu Zadavatel požaduje na straně AP podporu protokolů SSHv2 a SNMPv3.

Dodávané bezdrátové přístupové body musí být plně kompatibilní s dodávaným řadičem bezdrátové sítě.

16. Wi-Fi kontrolér

Zadavatel požaduje dodání bezdrátové sítě, která bude pracovat v centralizovaném režimu řízeném bezdrátovými řadiči (kontroléry). Dodávané kontroléry musí být plně kompatibilní s dodávanými AP.

Základní vlastnosti

Kontroléry musí podporovat standard bezdrátové komunikace IEEE 802.11ax s rozšířením do 6 GHz vysílacího pásma (Wi-Fi 6E) a umožnit zpětnou kompatibilitu se standardy IEEE 802.11a/b/g/n/ac.

Zadavatel požaduje dodání hardware zařízení, která budou mít minimálně 2 optické porty s volitelným fyzickým rozhraním o minimální rychlosti 10 Gbps a minimální propustnost kontroléru bude 20 Gbps. Je požadována podpora linkové agregace LACP, Rapid Spanning Tree protokolu a LLDP. Kontrolér musí podporovat řízení minimálně 500 AP a 10000 současně připojených klientů bez nutnosti přidání HW. Zadavatel požaduje zařízení velikosti 1 RU a možnosti montáže do standardního EIA rozvaděče o šířce 19” bez nutnosti použití dodatečných polic. Kontroléry musí být vybaveny redundantními zdroji napájení s možností výměny během provozu.

Pro zajištění vysoké dostupnosti služby je požadováno, aby kontroléry podporovaly práci v režimu active-active a active-standby. Výpadek aktivního kontroléru v redundantním páru nemá dopad na provoz již připojených klientů (není potřeba reautentizace na straně klientů). V rámci redundantního clusteru musí být umožněno sdílení licencí mezi kontroléry.

Bezpečnost

Pro dosažení vysokého stupně zabezpečení a s ohledem na možnost fyzického přístupu neoprávněných osob k bezdrátovými přístupovým bodům je požadováno, aby se AP pro připojení ke kontroléru ověřila certifikátem.

Do bezdrátové sítě Zadavatele budou připojena rozličná zařízení s rozdílnou podporou standardů bezdrátové komunikace a autentizačních mechanizmů. Z tohoto důvodu Zadavatel požaduje podporu starších autentizačních metod WPA/WPA2-PSK, WPA/WPA2-Enterprise, 802.1X, MAC autentizace, aplikační ověření – tzv. captive portál. Pro dodatečné zvýšení bezpečnosti autentizačních metod založených na sdílených klíčích je požadována možnost kombinace těchto metod s 802.1X (například s využitím MAC autentizace). Pro tzv. legacy zařízení, která jsou ve správě Zadavatele je požadována podpora autentizace pomocí několika různých klíčů na jednom SSID s ověřením klienta vůči RADIUS serveru, kdy klient je identifikován na základě MAC adresy. Kontroléry musí podporovat autentizaci dle nových standardů WPA3-Personal, WPA3-Enterprise a OWE. Pro zabezpečení komunikace s autentizačním serverem je požadována podpora RadSec protokolu (RADIUS over TLS).

Kontrolér musí podporovat RADIUS Accounting pro informování autentizačního serveru o aktuálním stavu sezení klientů a to včetně vyvolání tzv. RADIUS Interim Update v případě přepnutí klienta mezi AP.

Je požadována podpora autentizačních serverů RADIUS a LDAP. Pro možnost dynamické změny již autorizovaného klienta musí kontroléry implementovat tzv. Change of Authorization RFC 3576.

Kontrolér musí podporovat ochranu 802.11 řídicích rámců dle 802.11w a rozšířenou detekci útoků na bezdrátovou síť, tzv. Wireless Intrusion Prevention System. Kontroléry musí podporovat detekci škodlivých AP a omezení jejich vliv na bezdrátovou síť Zadavatele. Proto je požadována i implementace aktivní obrany proti útokům na bezdrátovou síť a to včetně metod deautentizace a tzv. tarpittingu (podvržení falešného kanálu nebo BSSID).

Řízení rádiového rozhraní

Řešení bezdrátové sítě musí být schopno automaticky reagovat na změny prostředí z pohledu šíření elektromagnetického záření detekované přímo jednotlivými AP nebo připojenými klienty. Je požadováno, aby kontroléry prováděly kontinuální měření vytíženosti vysílacích kanálů AP a detekci rušení signálu a upravovaly volby vysílacích kanálů včetně jejich šířky a vysílací výkon v koordinaci mezi AP. Kvůli elektromagnetickému rušení se specifickým časovým průběhem, vyvolávaném lékařskými diagnostickými přístroji, je nutné, aby bylo možno pro jednotlivá AP pozastavit proces automatických změn a zamezit tak nevýhodnému nastavení radiových parametrů pro dotčená AP. Pro zachycení periodicky se opakujících zdrojů rušení krátkých časových intervalů je nezbytné, aby systém umožňoval nastavit délku časového úseku měření v trvání alespoň 45 minut nebo zkrátit interval jednotlivých měření na délku 5 minut. Vyhodnocení takto získaných měření musí zohlednit data z okolních AP, aby prováděné optimalizační změny nastavení rádií jednotlivých AP nevyvolávaly opakované změny konfigurace a nedocházelo k cyklení. Z tohoto důvodu je požadováno, aby optimalizační změna rádiových profilů jednotlivých AP probíhala pouze mimo rozšířenou pracovní dobu trvající od 6 do 18 hodin.

Pro možnost analýzy problémů bezdrátové komunikace vzniklých rušením signálu je požadováno, aby kontroléry v součinnosti s AP podporovaly spektrální analýzu s možností časového záznamu do souboru a zpětné přehrávání záznamu.

Součástí řízení rádiového rozhraní je také podpora rychlého přepínání klientů mezi jednotlivými AP (Fast Transition dle IEEE 802.11r a OKC caching) a asistované rozdělení klientů mezi jednotlivá AP za účelem distribuce zátěže bezdrátové sítě. Je vyžadována podpora standardů IEEE 802.11u, 802.11v a 802.11k.

Funkce kontroléru

Kontroléry musí podporovat různé režimy přepínání provozu bezdrátových klientů a to režim tunelování provozu na kontrolér a per SSID lokálního přepínání rámců přímo na příslušném AP. Dále je požadována podpora L2 a L3 roamingu bez nutnosti instalace speciálního SW na klientovi.

Je požadováno, aby kontroléry umožnovaly statické směrování IPv4 a IPv6 paketů a dynamické směrování pomocí OSPF. Pro potřeby izolované návštěvnické sítě je vyžadována podpora lokálního DHCP serveru pro IPv4 a IPv6 a možnost překladu IP adres (PAT a NAT).

Kontroléry musí podporovat řízení AP v režimu MESH.

Je požadována podpora hostování captive portálů přímo na kontroléru pro účely autentizace přístupu do návštěvnické sítě. Kontrolér musí umožnit změnu vzhledu formuláře a mít implementováno rozhraní pro správu dočasných návštěvnických účtů.

Kontrolér musí implementovat zařazení klientských zařízení do tříd na základě typu nebo OS zařízení a následné uplatnění definovaných politik pro danou třídu.

Zadavatel požaduje, aby bylo možno prostřednictvím kontroléru provádět centrální správu, aktualizace, konfigurace vč. bezpečnostních politik a QoS profilů pro všechna AP. Je také vyžadována možnost automatického zablokování zařízení, které překračuje nastavitelné limity pro opakovanou neúspěšnou autentizaci nebo porušení bezpečnostní politiky.

Pro zařízení využívající protocol Bonjour je na straně kontroléru vyžadována podpora Bonjour brány, která detekuje dostupné služby a zajistí jejich distribuci mezi jednotlivé subnety s možností filtrování dostupnosti.

Správa

Vzdálená správa kontroléru bude probíhat šifrovanými aplikačními protokoly SSHv2, SCP a HTTPS, je také požadována podpora SNMPv3. Kontrolér musí podporovat aplikační rozhraní REST pro možnost automatizované správy.

Kontroléry musí umožnit zasílání servisních zpráv na více externích syslog serverů. Je požadována implementace diagnostických nástrojů ping, traceroute a test RADIUS spojení. Vzdálená správa musí být možná i s použitím IPv6 adresace.

Pro efektivní řešení problémů bezdrátové komunikace, bez nutnosti přítomnosti administrátora v místě instalace, je požadována podpora nástroje pro odchytávání bezdrátové komunikace a to včetně 802.11 hlaviček a možnost odeslání těchto dat do síťového analyzátoru typu Wireshark.

Pro minimalizaci dopadu aktualizace firmware je požadována možnost dopředného stažení firmware na skupinu či konkrétní AP (tzv. image pre-download).

17.Systém centrální správy sítě LAN/WLAN

V rámci obnovy síťové infrastruktury Zadavatel požaduje dodání nástroje na centrální správu síťových prvků, který bude kompatibilní s nabízenými AP, kontroléry a přepínači. Je požadováno, aby tento systém běžel jako virtuální appliance ve virtualizačním prostředí Zadavatele. Systém bude dodán ve formátu OVA, který poběží na platformě ESX/ESXi, a který musí obsahovat veškeré potřebné komponenty bez nutnosti pořizovat další licence např. pro operační systém databáze. V případě že toto není možné, musí být zajištěna dodávka redundantního řešení, která funkčně odpovídá VMware vMSC neuniformnímu clusteru včetně veškerého hardware, software a další infrastruktury.

Dodávaný nástroj umožní správu přístupových bodů AP, kontrolérů bezdrátové sítě a síťových přepínačů. Součástí dodávky musí být licence pro správu všech dodaných síťových prvků s možností flexibilního navyšování až do 4000 zařízení. Pro zjednodušení administrativní činnosti při přidávání nových síťových zařízení je požadována možnost manuální i automatické detekce síťových zařízení pomocí SNMP skenování definovaných IP rozsahů.

Přístup ke grafickému uživatelskému rozhraní bude prostřednictvím webového rozhraní s podporou protokolu HTTPS. Systém musí umožnit definování rolí síťových administrátorů na úrovni síťových zařízení a jejich funkcí.

Pro rychlé řešení problémů s připojením klientů do bezdrátové sítě je požadován real-time monitoring každého uživatele v síti včetně charakteristik jako jsou: kvalita RF signálu, využití pásma (in/out), stav ověření a čas, historie roamingu, délka trvání připojení, typ klientského zařízení, asociace s SSID, objem a seznam používaných L7 aplikací a navštívených webových kategorií. Nezbytná je dostupnost vyhledávání koncových uživatelů na základě MAC adresy, IP adresy, uživatelského jména a hostname zařízení. Uživatelské rozhraní systému umožní vizualizaci umístění prvků sítě v půdorysných mapách instalovaných lokalit. Dále je požadováno zobrazení bezdrátových klientů na mapě a jejich signálu a využívaných aplikací. Skrze mapové zobrazení systém umožní režim plánování rozmístění AP s vizualizací pokrytí signálem modelovaného prostředí.

Za účelem udržení konfiguračních standardů Zadavatel požaduje, aby systém podporoval tvorbu konfiguračních politik, které bude možné aplikovat na skupiny i jednotlivá zařízení. V systému musí být umožněno vytvoření konfiguračních šablon a to jak nových, tak jejich vytvoření kopií konfigurace běžícího zařízení. Je vyžadována podpora konfiguračních změn a upgrade firmware pomocí jednorázových nebo opakujících se pracovních úloh s možností plánování.

Pro úspěšné řešení problémů spojených se zásahy do konfigurace síťových zařízení je nezbytný proces auditu konfigurací. Dodávaný systém musí umožnit zálohu a archivaci konfigurací monitorovaných zařízení, porovnání rozdílů jednotlivých verzí konfigurací a také audit dle konfiguračních politik.

Systém musí umožnit nastavení prahových hodnot pro sledované veličiny síťových zařízení. Je vyžadováno, aby systém detekoval následující události: odchylka od vzorové konfigurace, RF metrika, objevení nového zařízení, objevení škodlivého AP, nadměrné vytížení AP (bandwidth), počet připojených klientů, nadměrná vytížení jedním klientem (bandwidth), počet zapnutí/vypnutí zařízení, počet zapnutí/vypnutí rádia, událost ze systému Intrusion Detection. Dalším důležitým mechanizmem je statistické monitorování a detekce síťových anomálií, jako například neobvyklé navýšení objemu provozu. V případě vzniku nestandardních stavů na monitorovaných zařízeních musí systém reagovat vygenerováním alarmu.

Pro kontinuální měření kvality sítě je požadována možnost monitorování stability a odezvy ostatních síťových služeb pro jednotlivé klienty jako je průměrný čas odpovědi DHCP, DNS či čas zpracování RADIUS autentizace.

Dodávaný nástroj musí umožnit vytváření reportů v PDF formátu shrnující různé přehledové statistiky o využití sítě a jejím stavu. Je požadována podpora automatického pravidelného generování reportů a jejich zasílání e-mailem.

18.Systém centrálního řízení přístupu do sítě LAN/WLAN

Zadavatel požaduje dodání systému centrálního řízení přístupu k síti, který naplňuje funkční model AAA – ověření, autorizace a účtování. Jedná se o klíčový prvek síťové infrastruktury, u kterého musí být zajištěna maximální dostupnost služby a vysoká úroveň zabezpečení.

Je požadováno dodání řešení, které bude plně redundantní minimálně o dvou instancích, kdy každá instance je schopna samostatně provádět ověřování, autorizaci a účtování bez ohledu na stav zbývajících instancí. Zadavatel umožňuje nasazení specializované hardware appliance nebo virtuální appliance, běžící ve virtualizačním prostředí Zadavatele (VMware ESX/ESXi), případně jejich kombinace. Z důvodu požadavků na vysokou dostupnost a citlivosti údajů zpracovávaných systémem musí dodané řešení fungovat zcela samostatně bez připojení do internetu.

Obecná charakteristika

Centralizovaný systém pro ověřování uživatelů, klasifikaci zařízení, řízení přístupu k síti pro interní uživatele i návštěvníky dle pravidel zohledňujících kontext připojení (identita uživatele, typ zařízení, místo a čas připojení apod.). Ve spolupráci s aktivními síťovými prvky (přepínači, bezdrátovými AP nebo řídícími kontroléry, VPN branami) poskytuje ochranu před neoprávněným přístupem k pevné datové síti, bezdrátové síti a k VPN připojení.

Zadavatel vyžaduje, aby dodávané řešení bylo možno prostřednictvím aplikačního rozhraní integrovat s externími bezpečnostními a analytickými systémy (například brána NGFW). Systém řízení přístupu do sítě může na základě sdílených informací koncové zařízení odpojit od sítě, omezit jeho přístup izolováním přesunem síťového segmentu nebo aplikováním filtrovacích pravidel, nebo napomoci v remediačním procesu.

Dodávané řešení musí umožnit distribuované nasazení jednotlivých instancí v různých lokalitách bez přímého propojení na vrstvě L2, možnost snadného přesunu instancí mezi lokalitami a rozšíření o další instance. Zároveň je kladen požadavek na snadné zálohování systému na aplikační úrovni a rychlou a úplnou obnovu konfigurace. Je požadováno řešení, které je dostupné ve formě hardware i software appliance podporovaných jedním výrobcem. Softwarová řešení musí být dostupné ve formě virtuálního serveru běžícího na platformách ESX nebo ESXi, na kterých je plně podporováno výrobcem.

Je požadována dodávka systému, který kapacitou systémových prostředků a licencí umožní aktivní 802.1X připojení minimálně 2000 klientů k datové síti.

Základní funkce AAA

Pro integraci řešení se stávajícími IT systémy na straně Zadavatele je požadována podpora autentizačního protokolu RADIUS pro ověření identity, autorizaci a účtování přístup k datové síti dle 802.1X. Systém musí umožnit vystupování v roli RADIUS proxy, kdy bude autentizační požadavky předávat na externí autentizační servery. S ohledem na množinu připojovaných zařízení v rámci Zadavatele je požadována implementace následujících autentizačních metod: MS-CHAPv2, EAP-MD5, Protected EAP (PEAP), EAP-TLS, PEAP-TLS, EAP-FAST a TEAP.

Jako zdroj identity musí dodávaný systém umožnit použít svou interní databázi, ve které lze modelovat uživatele i koncová zařízení s možností definice vlastních atributů. Dále je to adresářová služba dostupná prostřednictvím protokolu LDAP a její specifická varianta Microsoft Active Directory s umožněním autentizace uživatelským jménem a heslem. Pro Active Directory je vyžadována podpora více oddělených domén, které nejsou v jednom stromu a není mezi nimi navázána důvěra. Pro vícefaktorovou autentizaci je požadována podpora zdroje identity RADIUS Token (RFC 2865) a RSA RADIUS token server. Systém musí umožnit konfiguraci kombinací různých zdrojů identit pro různé autentizační scénáře včetně definice pořadí průchodů (např. AD -> lokální databáze).

Ověření identity uživatelů bude provedeno osobním certifikátem vystaveným certifikační autoritou Zadavatele, případně uživatelským jménem a heslem vůči adresářové službě nebo lokální databázi nebo kombinací metod. Identita koncového zařízení bude ověřena certifikátem (CA Zadavatele nebo CA výrobce), případně také uživatelským jménem a heslem nebo kombinací metod. Zařízení, která nepodporují autentizaci 802.1X, mohou být výjimečně ověřena pomocí tzv. MAC bypass autentizace. Je požadováno, aby tato nedostatečně průkazná metoda mohla být zkombinována s dodatečným ověřením např. kontrolou typu zařízení.

Za účelem provádění dodatečných ověření musí systém ve spolupráci se síťovou infrastrukturou podporovat rozpoznávání a klasifikaci připojených zařízení (PC, tiskáren, telefonů, tabletů, mobilních telefonů apod.) a to v rozsahu předpokládaných 2000 aktivních klientů. Systém musí umožnit vytváření a udržování profilů připojených zařízeních na základě informací jako jsou například hlavičky DHCP paketů, hlavičky HTTP paketů, prefix MAC adresy, stav zařízení apod.

Zadavatel požaduje, aby dodávaný systém umožnil autorizaci koncových zařízení a klientů nejen na základě jejich identity, ale i s využitím dodatečných informací jakými jsou členství uživatele nebo zařízení ve skupině v lokální databázi, profil zařízení, místo a čas připojení, historie připojení a stav zařízení. Výstupem autorizace bude RADIUS zpráva, jejíž atributy mohou obsahovat standardní i pro výrobce specifické atributy, jejichž hodnoty musí být možné dynamicky nastavit dle výsledku ověření / autorizace. Je požadováno, aby systém podporoval rozšíření změny autorizace ze strany RADIUS serveru - Change of Authorization (CoA, RFC 3576).

Zadavatel požaduje, aby proces ověření a autorizace byl na straně dodávaného systému modelován formou pravidel (politik) umožňujících hierarchické uspořádání a abstrakci s využitím pojmenovaných klasifikačních podmínek a návazných akcí. Systém musí umožnit správu pravidel v grafickém uživatelském rozhraní, které pro přístup nevyžaduje instalaci specializovaného software (těžký klient). V rámci redundantního řešení musí být veškerá konfigurace i lokální databáze identit automaticky synchronizována mezi všemi instancemi a zároveň systém umožní přístup k záznamům o průběhu ověřování a účtování ze všech instancí prostřednictvím jedné instance.

Pro účely bezpečnostní analýzy je požadováno, aby byl průběh přístupu koncového klienta k datové síti zaznamenán a průběžně aktualizován a proto je nutné, aby dodávaný systém podporoval zaznamenávání tzv. RADIUS accounting zpráv.

Pro účely řešení problémů s ověřováním a autorizací musí být všechny události vzniklé interakcí autentizátoru a RADIUS serveru zaznamenány do databáze a zpřístupněny v grafickém administrátorském rozhraní systému včetně možnosti filtrace a vyhledávání v těchto záznamech. Dále je požadována podpora SNMPv3 protokolu pro monitorování stavu autentizačního systému, NTP protokolu pro synchronizaci systémového času a podpora SMTP protokolu pro zasílání e-mailových notifikací. Dodávané řešení musí zaznamenávat události (varování, chyby) do systémového logu, který je přístupný a řešení musí umožnit zasílání systémových logů na externí syslog server. Pro analýzu problémů síťové komunikace mezi autentizačním serverem a síťovými zařízeními je požadována možnost zachycení síťového provozu na straně autentizačního serveru (packet capture).

Podpora přístupu pro návštěvníky

Zadavatel hodlá zpřístupnit bezdrátovou síť návštěvníkům nemocničních zařízení za účelem umožnění přístupu do veřejného internetu. Přístup k této síti je specifický množstvím a různorodostí klientů, jejichž identitu nelze vůbec nebo jen částečně ověřit. S ohledem na možné komplikace a omezení, která by si vyžádalo nasazení 802.1X ověřování se Zadavatel rozhodl pro autorizaci přístupu na základě uživatelského vyplnění registračního formuláře prostřednictvím tzv. Captive portálu. Zadavatel proto požaduje, aby dodávaný systém řízení přístupu k síti implementoval funkci Captive portal a funkci portálu pro správu uživatelských účtů včetně správy databáze návštěvnických účtů.

Systém musí umožnit vytváření časově omezených oprávnění pro přístup k síti pro návštěvníky, externí spolupracovníky apod. a to jak pro přístup k bezdrátové, tak i pevné síti LAN. Je požadována možnost definice více typů návštěvnických účtů dle vztahu uživatelů k Zadavateli a to včetně možnosti potvrzení přístupu pracovníkem Zadavatele (tzv. sponzoring). Každý typ účtu může mít jinou délku

platnosti a získat jiný přístup k síti. Dodávaný systém musí zpřístupnit jednoduchý webový portál pro správu těchto účtů. Služby portálu budou využívat osoby pověřené Zadavatelem a bude se jednat o administrativní pracovníky s omezenou znalostí IT prostředí. Dále je požadováno, aby systém umožnil vytvoření samoobslužného registračního portálu, který budou využívat přímo návštěvníci. Zadavatel požaduje možnost vytvoření více registračních portálů za účelem oddělení správy návštěvníků a externích pracovníků, kdy každou doménu bude spravovat jiná skupina administrativních pracovníků. Systém musí umožnit snadnou editaci požadovaných položek a vzhledu registračních formulářů prostřednictvím grafického rozhraní integrovaného do management rozhraní.

Systém musí umožnit integraci s externími e-mail a SMS branami pro automatizaci zasílání přístupových údajů vytvářeným uživatelům. Požaduje se, aby webová rozhraní byla dostupná přes HTTP i HTTPS protokoly.

Požaduje se, aby řešení přístupu pro návštěvníky bylo součástí dodávané appliance bez nutnosti instalace dodatečného software. Součástí dodávky musí být všechny potřebné software komponenty a licence pro tvorbu sponzorských portálů, captive portálů, registračních formulářů.

Řízení přístupu ke správě zařízení

Pro omezení přístupu ke správě infrastruktury jen pro oprávněné administrátory a za účelem auditování prováděných činností je vyžadována implementace protokolu RADIUS i TACACS+. Systém musí umožnit ověření identity administrátora, provádět autorizace jednotlivých příkazů a uchovávat historii provedených příkazů (včetně zamítnutých). Pro jednoduchou správu oprávnění Zadavatel požaduje možnost tvorby administrátorských rolí, u kterých budou specifikována pravidla povolených příkazů pomocí regulárních výrazů. Při přístupu ke kritickým prvkům infrastruktury je vyžadováno, aby systém podporoval možnost dvoufaktorového ověření (například jméno a heslo, token).

Stejně jako v případě služby RADIUS serveru, musí být ověřování protokolem TACACS+ dostupné na všech instancích dodávaného systému a spravované centrálně prostřednictvím grafického uživatelského rozhraní. Zadavatel požaduje, aby funkcionalita TACACS+ byla součástí appliance a nebylo třeba instalace dodatečného software. Součástí dodávky musí být i případné licence na řízení přístupu pro 500 zařízení.

Další vlastnosti

Pro tvoru detailních autorizačních pravidel musí systém umožnit vyčítání definovaných atributů objektu uživatele z Active Directory. Pro výše zmíněnou integraci s externími bezpečnostními nástroji je požadována dostupnost otevřeného aplikačního rozhraní pro oboustrannou komunikaci (sdílení informací a signalizace z/do externích systémů, rychlou a automatizovanou karanténu, apod.). Dodávaný systém musí být certifikován FIPS 140-2 a musí podporovat aktivaci FIPS módu, který automaticky zakáže nepovolené autentizační protokoly.

19. Příslušenství pro síťové technologie

- Pro všechna síťová zařízení je potřeba zajisti pro každý SFP+/QSFP/SFP28/SFP56/QSFP28 či FC HBA patřičný multimode nebo singlemode transceiver (dle skutečné situace) a patch kabel. Patch kabely budou vždy vedeny nad anebo pod rozvaděči. Odhadovaná potřebná délka patch kabelů je 5 metrů.
- Pokud není k dispozici kabelový žlab, je nutné, aby si jej Dodavatel pro účel propojení racků a technologií dodělal.

- Racky jsou v různém technickém stavu a je nutné počítat s omezeným prostorem a omezenou nosností racků. Hloubka serverových racků je vždy nejméně 800 mm. Zadavatel se nebrání dodávce nových racků Dodavatelem. V případě dodávky nového racku je na Dodavateli zajištění kabeláže do úrovně nadřazeného elektrického rozvaděče. Elektrická kabeláž musí zahrnout také ochranné lišty a požární ucpávky.
- Součástí dodávky musí být také patřičné napájecí kabely.
- Součástí každého zařízení musí být ližiny pro montáž do 19“ racku. Pokud to obsluha zařízení vyžaduje, musí být ližiny vysouvací.

20. Implementace

Zadavatel ve vzorové tabulce, uvedené v této kapitole, popisuje minimální nutné kroky k nasazení jednotlivých technologií i celků. Zadavatel očekává, že tyto dílčí kroky budou součástí sledovaných kroků v rámci projektového řízení. Dodavatel musí splnit dodání těchto částí pomocí realizačního týmu, kdy seznam členů realizačního týmu je součástí předložené nabídky Dodavatele k příslušné části veřejné zakázky. V případě jakékoliv změny v realizačního týmu, dodavatel musí zajistit plnění kvalifikačních kritérií uvedených v zadávacích podmínkách po celou dobu realizace veřejné zakázky. Všechny implementační činnosti musí být realizovány uvedeným realizačním týmem (dle kvalifikačních předpokladů). Člověkoden je uveden jako 7,5 pracovní hodiny. Zadavatel konstatuje, že činnosti mající přímý dopad do rutinního provozu Zadavatele, bude nutné vykonávat mimo běžnou pracovní dobu, tj. v nočních hodinách případně o víkendech.

Každý technologický celek bude mít doloženy nejméně tyto dokumenty před zahájením samotné implementace:

a) Dokument popisující obsah implementace (SoW), který obsahuje:
   - popis implementace technického řešení,
   - adresní informace,
   - navrženou topologii (L1-L3 dle modelu ISO-OSI),
   - harmonogram,
   - spoluúčast Zadavatele a kontaktní matici Dodavatele.

SoW musí popisovat co možná bezvýpadkovou migraci mezi prostředími (původní -> nové).

b) Návrh akceptačních testů obsahujících ověření měřitelných hodnot v této zadávací dokumentaci.

c) Online provozní prostředí umístěné buď v prostředí Zadavatele, nebo prostředí Dodavatele. Prostředí musí mít nejméně: Intranet zajišťující komunikaci mezi Dodavatelem a Zadavatelem v reálném čase formou „interní wikipedie“, CMDB, Helpdesk a monitoring nástroj. Všechny nástroje musí být integrovány do jednoho prostředí a obsahovat všechny komponenty všech nabízených technologických celků.

Technologický celek	Technologie	Činnost	Počet člověkodní
A) Technologie datového centra	Velké výpočetní servery (per ks)	Zahoření technologie, upgrade firmware na poslední verzi a montáž do racků.	
		Instalace vSphere, integrace s vCenter a nasazení bezpečnostních funkcí.	
		Migrace VM s volitelnou reinstalací. Zadavatel rozhodne, zda-li bude konkrétní VM reinstalována, nebo pouze migrována.	
	Malé výpočetní servery (per ks)	Zahoření technologie, upgrade firmware na poslední verzi a montáž do racků.	
		Instalace vSphere, integrace s vCenter a nasazení bezpečnostních funkcí.	
		Migrace VM s volitelnou reinstalací. Zadavatel rozhodne, zda-li bude konkrétní VM reinstalována, nebo pouze migrována.	
	Velké blokové diskové pole (per pár)	Zahoření technologie, upgrade firmware na poslední verzi a montáž do racků.	
		Konfigurace RAID, LUN a konfigurace pro všechny hosty (stávající a nové).	
		Výkonnostní testy.	
	Střední blokové diskové pole (per ks)	Zahoření technologie, upgrade firmware na poslední verzi a montáž do racků.	
		Konfigurace RAID, LUN a konfigurace pro všechny hosty (stávající a nové).	
		Výkonnostní testy.	
	Malé blokové diskové pole (per ks)	Zahoření technologie, upgrade firmware na poslední verzi a montáž do racků	
		Konfigurace RAID, LUN a sestavení non-uniform vMSC pro všechny hosty (stávající a nové).	
		Výkonnostní testy.	
	Fibre channel přepínače (volitelně, per pár)	Zahoření, upgrade, firmware nastavení centrálního managementu, konfigurace ISL trunků a zoningu.	
		Výkonností a akceptační testy.	
	Příslušenství pro datacenterové technologie (per site)	Patchování, vyvázání do racku, označení veškeré kabeláže.	
	Licence pro MS Windows server 2022 CAL (per položka)	Dodávka licencí.	
	Licence pro další VMware technologie (per položka)	Nasazení, upgrade a optimalizace vCenter platforem zákazníka.	
	Páteřní přepínače (per pár)	Upgrade firmware, konfigurace LACP-MLAG, re-segmentace LAN, rozdělení broadcast domén, nasazení V(X)LAN, nasazení autorizačního konceptu a testování redundance.	
	Akceptační testy (per technologický celek)	Testy naplnění uvedených výkonnostních parametrů (pří neúspěšném testu je test	

		opakován, toto není zahrnuto v odhadu pracnosti).	
	Dokumentace (per technologický celek)	Předání administrátorské a uživatelské dokumentace.	
B) Technologie zálohování	Diskové pole pro nestrukturovaná data (per cluster)	Upgrade firmware, zahoření platforem.	
		Integrace API platforem se zálohovacím software a snapshoty blokových diskových polí.	
		Integrace s MS AD a PKI	
		Integrace s AV-XDR platformou	
	Zálohovací a infrastrukturní server	Upgrade firmware, zahoření platforem, instalace OS a instalace managementu zálohovacího software.	
	Licence na zálohovací software (per 30 VM)	Návrh plánu záloh a obnov pro všechna aktiva - servery. Aktiva budou klasifikována dle standardu určeného Zadavatelem. Bude vypracována formální dokumentace popisující plán záloh a obnov včetně nastavení procesu kontroly aplikační konzistence záloh a průběhu zálohování. Bude nastaven plán pravidelné antivirové kontroly obsahu záloh. Všechny formální požadavky budou také nakonfigurovány na diskovém poli pro nestrukturovaná data, zálohovacím software a AV-XDR sofware.	
		Testování obnovy.	
		Testování odolnosti proti úniku zálohovaných dat, testování autorizace mezi zdrojem a cílem záloh.	
	Pásková knihovna (per ks)	Nasazení páskové knihovny, konfigurace mechanik a archivačních procesů dle pravidel, které určí Zadavatel.	
	Příslušenství pro datacenterové technologie (per site)	Patchování, vyvázání do racku, označení veškeré kabeláže.	
	Akceptační testy (per technologický celek)	Testy naplnění uvedených výkonnostních parametrů (pří neúspěšném testu je test opakován, toto není zahrnuto v odhadu pracnosti).	
	Dokumentace (per technologický celek)	Předání administrátorské a uživatelské dokumentace.	
C) Technologie přístupu	Licence pro VDI technologii (per lokalita)	Vytvoření návrhu aplikačních profilů pro VDI prostředí.	
		Konfigurace aplikační profilů VDI prostředí a integrace s AD a PKI infrastrukturou.	
		Konfigurace vzdáleného přístupu k VDI technologiím a kryptografie.	
		Migrace aplikací do VDI prostředí.	

		Ladění a optimalizace provozních problémů jednotlivých aplikací.	
	Přístupové přepínače (všechny typy, per ks)	Upgrade firmware, konfigurace LACP-MLAG, konfigurace přístupových bezpečnostních funkcí, konfigurace V(X)LAN, konfigurace autorizačního konceptu a testování redundance.	
	Bezdrátové přístupové body (per ks)	Upgrade firmware a registrace AP v centrálním kontroléru.	
	Řadič bezdrátové sítě (per pár)	Upgrade firmware, konfigurace active-active clusteru kontrolérů, konfigurace LAN, konfigurace SSID, konfigurace kryptografie, optimalizace konfigurace přenosového pásma.	
	Systém centrální správy LAN/WLAN (per projekt)	Konfigurace centrálního managementu, konfigurace profilů pro jednotlivá zařízení, konfigurace L7 inspekce provozu, konfigurace interaktivních map s lokalizací bezdrátových klientů.	
	Systém centrální správy identit pro přístup do sítě LAN/WLAN (per site)	Konfigurace systému centrální správy identit a řízení přístupu k LAN-WLAN.	
		Vytváření profilů pro jednotlivé typy zařízení a softwarové výbavy.	
		Konfigurace přístupových politik pro jednotlivá zařízení a následných akcí (přiřazení VLAN, izolace apod.).	
		Optimalizace provozních problémů jednotlivých politik a řešení problémů suplikantů.	
		Konfigurace webového portálu pro hosty (vytvoření webové přístupové stránky dle požadavků Zadavatele).	
	Akceptační testy (per technologický celek)	Testy naplnění uvedených výkonnostních parametrů (pří neúspěšném testu je test opakován, toto není zahrnuto v odhadu pracnosti).	
	Dokumentace (per technologický celek)	Předání administrátorské a uživatelské dokumentace.	

21. Četnost komponent v jednotlivých zdravotnických zařízeních

Seznam požadovaného počtu komponent v jednotlivých nemocnicích je detailně rozpracován v dokumentu „Příloha č1 – Krycí_list_KB_infra“.