# Storage systém s podporou S3, CIFS a NFS pro vysokou ochranu dat

## Úvod

* Toto technické zadání specifikuje požadavky na dodávku a implementaci úložiště podporujícího primárně protokol S3 a sekundárně CIFS a NFS. Úložiště bude rozděleno do dvou boxů ve dvou geograficky oddělených lokalitách propojených dedikovaným IP spojením. Kapacita řešení bude celkově 300 TiB (čistá kapacita bez komprese, deduplikace a pod.). Řešení složené ze dvou nodů, umístěných každý v samostatné lokalitě propojené dedikovaným IP spojením. Lokality vzdálené cca 2km. IP spoj zajistí na svých prostředcích zadavatel.

## Požadavky na hardware na jeden node úložiště

* NVMe architektura.
* Možnost rozdělení kapacity na samostatné logické celky (např. jeden box 240TiB rozdělených na 60TiB pro provozní data a 180TiB pro data záloh a druhý box 60 TiB pro provozní data; provozní data mezi boxy budou replikována).
* Všechny HW komponenty budou v konfiguraci vysoké dostupnosti.
* Podpora scénáře rozšiřování kapacity prostřednictvím pořízení dalších boxů bez nutnosti změny konfigurace zálohovacího řešení (transparentní rozšíření kapacity S3 storage repository - bucketu). Rozšiřitelnost minimálně na 1PiB.
* Možnost škálování (rozšiřování) řešení i z pohledu výkonu řešení (zvýšení počtu IOPs bucketu např. doplněním dalších HW komponent nebo další nodů).
* Minimální celkový výkon jednoho nodu musí být alespoň min 80K IOPS při 32KB bloku, protokolu NFS, poměru 80/20% write/read sekvenčních operací, s průměrnou latencí do 2ms.
* Upgrade software a hardware u řadičů je proveditelný za chodu a bez ztráty přístupu k datům.
* Podpora asynchronní replikace dat pro svazky publikované pomocí protokolu NFS,S3 i CIFS
* Provedení rackmount 19“, max 4U

## Podporované protokoly

* Primární: S3 (kompatibilní s AWS S3 API)
* Sekundární: CIFS (pro Windows-based prostředí), NFS (pro Linux/Unix prostředí)

## Poptávané úlohy/scénáře

Řešení musí podporovat následující úlohy a jejich minimální parametry:

* Zálohování dat pomocí Veeam:
  + Rychlost záloh minimálně 1GBps
  + Možnost generační obměny HW (disků, řadičů) při zachování zámků nad uloženými objekty
* Ukládání a čtení dat v provozních úlohách, typicky úloha perzistentního S3 úložiště souborů (obrazy, dokumenty) pro webovou aplikace v Kubernetes clusteru:
  + Vysoká dostupnost (nezávislost na stavu jednoho z HW zařízení)
  + Latence práce s jedním objektem:
    - Čtení (GET): max 10 ms
    - Zápis (PUT): max 20 ms, zejména pokud je objekt menší než 1 MB.
    - Mazání (DELETE): max 5 ms.

## Síťové požadavky

* Možnost propojení boxů prostřednictvím dedikovaného IP spojení.
* Propojení prostřednictvím minimálně 4 x 25/10Gbps Ethernet portů typu SFP28 (v každém nodu) s možností agregace linek, včetně dodávky SFP28 zářičů.
* Možnost připojení do lokálních sítí v obou lokalitách

## Bezpečnost a ochrana dat

* Podpora šifrování dat při přenosu (zabezpečený síťový přenos dat) i při uložení (šifrování jak na úrovni celých disků, tak na aplikační úrovni vybraných logických celků/oddílů dat)
* Všechny šifrovací či kryptografické funkce, mechanizmy, algoritmy a prostředky musí být v souladu s doporučením Národního úřadu pro kybernetickou a informační bezpečnost (NUKIB) v aktuálním znění (dokument [Doporučení v oblasti kryptografických prostředků](https://nukib.gov.cz/cs/infoservis/doporuceni/)). Za soulad se považuje použití pouze schválených kryptografických prostředků.
* Dostupnost dat pro všechny protokoly/úlohy i v případě nedostupnosti jednoho nodu.
* Ochrana dat prostřednictvím verzování a imutability - zamykání jak logických celků, tak vybraných uložených záloh dat (snapshotů) proti přepsání či smazání (WORM funkcionalita).
* Datové úložiště musí podporovat vytváření snapshotů logických svazků a jejich publikaci pro čtení i zápis
* Funkce koše – možnost časově omezeného obnovení smazaných objektů
* Podpora ochrany před útoky typu ransomware na úrovni souborového přístupu k datům. Ochrana principiálně spočívá ve vytvoření snapshotu uzamčeného proti změnám při detekci útoku.
* Multiadministrátorské schválení - schvalování kritických či destruktivních aktivit více uživateli zároveň.
* Cache pro zápis musí být replikována a zálohována mezi oběma boxy, aby se zabránilo ztrátě dat v případě selhání boxu nebo výpadku napájení
* Datové úložiště musí mít vyčleněn alespoň jeden spare disk; podpora RAID s dvojitou paritou, odolný proti výpadku dvou ks disků
* Podpora multitenantnosti, kde lze na storage tenant nastavit dedikované přístupové IP adresy, administrátory, přístupové účty a sety přístupových protokolů
* Možnost nastavení přístupových práv na úrovni protokolu S3, CIFS a NFS
* Automatické zálohování do druhé lokality
* Podpora autentizace uživatelů daného tenantu přistupujících k datům prostřednictvím protokolů:
  + MS AD/LDAP (pro CIFS i NFS) a Kerberos (pro NFS)
  + Access Key a Secret Key (pro S3)
* Podpora autentizace administrátorů daného tenantu (přístup k administračnímu rozhraní) prostřednictvím protokolů:
  + MS AD/LDAP/Kerberos
  + SAML 2.0/OIDC
  + Úložiště musí podporovat vícefaktorovou autentizaci.
* Podpora logování a sledování auditní stopy – úložiště musí zaznamenávat logy a auditní stopu tak, aby měly tyto informace vypovídající hodnotu pro řešení a forenzní analýzu kybernetických bezpečnostních událostí a aby byly jednoduše integrovatelné na centrální nástroj pro sběr a analýzu těchto dat. Musí splňovat následující požadavky:
  + Logy musí obsahovat minimálně tyto události:
    - přihlášení a odhlášení všech uživatelů/administrátorů či jiných privilegovaných účtů,
    - činnosti provedené administrátory, např.:
      * přidělení/odebrání oprávnění,
      * založení/smazání uživatele
      * přidělení/odebrání role
      * reset hesla (pokud je prováděn na úrovni logujícího informačního aktiva)
      * povýšení oprávnění administrátora, převzetí role
      * změna konfigurace logovacího mechanizmu
      * změna konfigurace informačního aktiva,
    - automatická informační, varovná a chybová hlášení provozního charakteru
    - záznamy o manipulaci s daty (informace o objektu a druhu operace s ním)
  + Podpora protokolu syslog pro přenos logů do centrálního úložiště provozovaného zadavatelem a SMTP pro zasílání notifikací systému
* Podpora SNMPv3 protokolu pro monitoring
* Na základě analýzy rizik je použití technických nebo programových prostředků následujících výrobců, včetně jejich dceřiných společností, v tomto řešení vyloučeno:
  + Huawei Technologies Co., Ltd., Šen-čen, Čínská lidová republika
  + ZTE Corporation, Šen-čen, Čínská lidová republika

## Integrace se SW Veeam

* Podpora nativní integrace se zálohovacím softwarem Veeam
* Možnost optimalizace zálohování a obnova na základě požadavků Veeam

## Další požadavky

* Podpora správy a monitoringu prostřednictvím webového rozhraní
* Poskytnutí návodů a školení pro administrátory
* Možnost budoucího rozšíření kapacity
* SLA na úrovni 99,9 % dostupnosti
* Záruka 5 let

## Akceptační testy

* Ukázka celkového IOPs výkonu dle požadavků zadání
* Ukázka konfigurace S3 bucketu včetně jeho připojení do Veeam infrastruktury zadavatele
* Ukázka nastavení a ověření funkčnosti verzování a zamykání na úrovni S3
* Nastavení a otestování oprávnění RBAC
* Ukázka zálohování provozních dat uložených v S3 úložišti do jiného storage prostředí

## Harmonogram

Dodávka hardware do 120 dnů od účinnosti smlouvy

Zprovoznění do 30 dnů od dodání

Testovací provoz po dobu 14 dnů

Předání do ostrého provozu po úspěšném testování (provedení akceptačních testů)

## Požadované dokumenty

* Technická specifikace nabízeného řešení
* Dokumentace k implementaci a správě systému
* Výsledky testovacího provozu