

Specifikace plnění – IPAM (IP address management)

Typ řešení: **Centralizovaný systém pro správu IP adresního rozsahu, rozdělitelný do několika částí, např.: koncová zařízení vs datová centra**

1. Základní parametry:

- Provoz řešení v prostředí on-premise virtualizované infrastruktury;
- Řešení musí podporovat provoz v režimu vysoké dostupnosti (High Availability);
- Podpora správy IPv4 a IPv6 adresního prostoru;
- Hierarchická správa adresních rozsahů a podsítí;
- Správa VLAN a VRF;
- Řešení musí umožňovat definici uživatelsky rozšiřitelných atributů (Custom Fields) u spravovaných objektů;
- Řešení musí podporovat správu životního cyklu IP adres, včetně rezervace, přidělení a uvolnění adres;
- Automatická kontrola duplicitních IP adres a překryvů podsítí;
- Network Discovery prostřednictvím ICMP, SNMP a ARP;
- Plánování a spouštění Discovery nad jednotlivými síťovými segmenty;
- Porovnání zjištěného stavu s evidovanými daty;
- Řešení musí poskytovat standardizované REST API pro integraci s externími systémy a automatizačními nástroji;
- Řešení musí podporovat integraci s adresářovou službou Microsoft Active Directory;
- Řešení musí podporovat vícefaktorovou autentizaci (MFA), je-li využívána v prostředí zadavatele - volitelné;
- Řešení musí podporovat řízení přístupových oprávnění na základě rolí (RBAC);
- Integrace se stávajícími Microsoft DNS/DHCP a BIND/ISC DHCP;
- Export dat ve standardizovaných formátech xls/xlsx/csv;
- Transparentní licenční model bez dodatečných licenčních poplatků za požadované funkcionality;
- Softwarová podpora výrobce nebo výrobcem autorizovaného partnera po dobu 60 měsíců;
- Technická podpora musí zahrnovat přístup k opravám, novým verzím software, aktualizacím a bezpečnostním záplatám vydaným výrobcem v rámci poskytované podpory. Případně dodavatel může navrhnout jiný model podpory;
- Provoz řešení v prostředí on-premise virtualizované infrastruktury;
- Součástí dodávky jsou veškeré potřebné licence pro zajištění funkcionality řešení, dle této specifikace.

2. Architektura řešení

- Řešení musí představovat centrální autoritativní registr (Single Source of Truth) pro správu IP adresního prostoru.
- Řešení musí umožňovat správu minimálně 150 000 IP adres s kapacitní rezervou odpovídající předpokládanému rozvoji prostředí zadavatele;
- Řešení musí podporovat správu IPv4, IPv6, podsítí, VLAN, VRF a souvisejících síťových objektů;
- Řešení musí umožňovat evidenci síťových lokalit, organizačních jednotek a dalších logických struktur souvisejících se správou adresního prostoru;
- Řešení musí podporovat vyhledávání, filtrování a třídění objektů podle evidovaných atributů;
- Řešení musí umožňovat správu adresních rozsahů bez omezení jejich hierarchické struktury;
- Řešení musí podporovat delegovanou správu adresních rozsahů při zachování centrální evidence;
- Řešení musí umožňovat podporu schvalovacích procesů při správě adresního prostoru;

- Součástí řešení musí být automatická kontrola konzistence adresního prostoru a identifikace duplicitních nebo kolidujících záznamů;
- Řešení musí poskytovat grafické uživatelské rozhraní pro správu adresního prostoru.

3. Implementace, import dat a discovery

- Implementace řešení a její předpokládaný rozsah dle rozsahu mandays je součástí dodávky;
- Součástí implementace je instalace, konfigurace, integrace, import dat, uvedení systému do provozu a ověření jeho funkčnosti;
- Dodavatel zajistí analýzu, konsolidaci a validaci dat určených k importu;
- Součástí dodávky je import stávajících dat do systému IPAM;
- Před produkčním importem bude proveden testovací import dat;
- Po dokončení importu bude provedeno ověření správnosti a úplnosti importovaných dat;
- Součástí řešení musí být funkce Network Discovery;
- Discovery musí podporovat ICMP, SNMP a ARP;
- Discovery musí umožňovat plánované i manuální spouštění jednotlivých úloh;
- Discovery musí umožňovat skenování jednotlivých síťových segmentů;
- Discovery musí umožňovat porovnání skutečného stavu s evidovanými daty;
- Discovery musí umožňovat identifikaci nových zařízení, nevyužívaných IP adres, konfliktů IP adres, překryvů podsítí a dalších nekonzistencí;
- Discovery musí umožňovat získávání dostupných informací o síťových zařízeních prostřednictvím podporovaných komunikačních protokolů.

4. Bezpečnost, Logování a prostředí

- Veškeré administrátorské operace musí být zaznamenávány do auditního logu, který musí umožňovat dohledání historie provedených změn;
- Auditní záznamy musí být chráněny proti neoprávněné změně nebo odstranění.
- Řešení musí podporovat bezpečný export provozních a auditních událostí do centrálních dohledových systémů zadavatele prostřednictvím standardizovaných zabezpečených rozhraní.
- Řešení musí umožňovat napojení na stávající Log management a SIEM
- Řešení musí podporovat zálohování databáze a aplikační konfigurace.
- Řešení musí podporovat bezpečnostní požadavky zadavatele vyplývající ze zákona o kybernetické bezpečnosti, požadavků NIS2 a souvisejících bezpečnostních předpisů.

5. Specifikace hardware

- Dle uvážení dodavatele

6. Dokumentace

Prodávající je povinen předat Kupujícímu kompletní dokumentaci v českém jazyce, která je nutná k převzetí a k užívání řešení, a to minimálně v tomto rozsahu:

- technickou dokumentaci Software;
- administrátorskou dokumentaci;
- uživatelskou dokumentaci;
- licenční dokumentaci;
- dodací list;
- další dokumenty potřebné k užívání Hardware či Software

7. Školení

- Zaškolení administrátorů v oblasti administrace, konfigurace, provozu a diagnostiky systému IP Address Management a uživatelů v rámci užívání.
- Případně modul školení navržené dodavatelem v rozsahu administrátor a uživatel.

