

**Klasifikace: Veřejný dokument**

Příloha č. 1 Zadávací dokumentace

Technická příloha – specifikace technických požadavků pro Zadávací ŘÍZENÍ centralního LOG managementu

Obsah

[1 Verze dokumentu 3](#_Toc98762576)

[2 Seznam zkratek 4](#_Toc98762577)

[Computer security incident response team 4](#_Toc98762578)

[Česká státní norma 4](#_Toc98762579)

[Garant podpůrného aktiva 4](#_Toc98762580)

[3 Úvod 7](#_Toc98762581)

[3.1 Předmět plnění veřejné zakázky 7](#_Toc98762582)

[4 Současný stav a popis prostředí 8](#_Toc98762583)

[4.1 Souhrnné objemy logů 8](#_Toc98762584)

[4.2 Specifické aplikace SŽ 9](#_Toc98762585)

[4.3 Generické systémy a aplikace 10](#_Toc98762586)

[4.3.1 Doménové řadiče, operační systémy, služby 10](#_Toc98762587)

[4.3.2 Síťové technologie 15](#_Toc98762588)

[4.4 Bezpečnostní technologie 17](#_Toc98762589)

[5 Požadavky CLM 18](#_Toc98762590)

[5.1 Funkční požadavky 18](#_Toc98762591)

[5.2 Architektura řešení 21](#_Toc98762592)

[5.3 SW a HW 22](#_Toc98762593)

[5.4 Zajištění vysoké dostupnosti 23](#_Toc98762594)

[5.5 Integrace 23](#_Toc98762595)

[5.6 Požadavky dle § 22 vyhlášky č. 82/2018 24](#_Toc98762596)

[5.6.1 Bezpečnostní monitoring jako součásti CLM 26](#_Toc98762597)

[5.7 Počet uživatelů CLM 27](#_Toc98762598)

[6 Požadavky na dodávku 28](#_Toc98762599)

[6.1 Analýza 28](#_Toc98762600)

[6.2 Definice Technického návrhu implementace 28](#_Toc98762601)

[6.3 Dodávka SW, HW a licencí 31](#_Toc98762602)

[6.3.1 Dodávka HW 31](#_Toc98762603)

[6.3.2 Dodávka SW a licencí 31](#_Toc98762604)

[6.4 Dodávka Produkčního a testovacího prostředí 32](#_Toc98762605)

[6.5 Instalace 32](#_Toc98762606)

[6.6 Konfigurace 32](#_Toc98762607)

[6.7 Testování 33](#_Toc98762608)

[6.7.1 Funkční testy 33](#_Toc98762609)

[6.7.2 Zátěžové testy 33](#_Toc98762610)

[6.7.3 Bezpečnostní testy 33](#_Toc98762611)

[6.7.4 Sken zranitelností 34](#_Toc98762612)

[6.7.5 Testy zajištění kontinuity 34](#_Toc98762613)

[6.8 Pilotní provoz 34](#_Toc98762614)

[6.9 Dokumentace 35](#_Toc98762615)

[6.10 Školení 36](#_Toc98762616)

[6.11 Předání do provozu 36](#_Toc98762617)

[6.12 Zajištění technické podpory provozu 36](#_Toc98762618)

[6.13 Nadstandardní služby 37](#_Toc98762619)

# Verze dokumentu

|  |  |  |  |
| --- | --- | --- | --- |
| Verze dokumentu | Datum | Autor | Změny |
| 5.00 | 20.1.2022 | Správa železnic |  |

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| Zkratka | Popis |
| AD, MS AD | Microsoft Active Directory |
| ATP/ATI | Advanced Threat Protection |
| AKB | Architekt kybernetické bezpečnosti |
| API | Rozhraní pro programování aplikací (Application Programming Interface) |
| BU | Bezpečnostní událost |
| CA | Certifikační autorita |
| CERT | Computer emergency response team |
| CISO | Manažer informační bezpečnosti (Chief Information Security Officer) |
| CMDB | Konfigurační databáze (Configuration Management Database) |
| CSIRT | Computer security incident response team |
| ČSN | Česká státní norma |
| CLM, CLS | Centrální Log Management, Centrální logovací systém |
| DLP | Data Loss Prevention |
| EPS | Počet událostí za sekundu (Events per Second) |
| GPA | Garant primárního aktiva |
| GPdA | Garant podpůrného aktiva |
| HA | Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance |
| Hardening | Hardening je proces zabezpečení konfigurace systému takovým způsobem, který omezí výskyt zranitelností využitelných útočníkem |
| HIPS | Host Intrusion Prevention System |
| HW | Hardware |
| ICT | Informační a komunikační technologie (Information and Communication TechnoLogies) |
| IDM | Správa uživatelských účtů (Identity Management) |
| IS | Informační systém |
| ISVS | Informační systémy veřejné správy |
| ITSM | IT Service Management |
| KBI | Kybernetický bezpečnostní incident |
| KII | Kritická informační infrastruktura |
| LDAP | Lightweight Directory Access Protocol |
| LLD | Nízko úrovňový design (Low Level Design) |
| MB | Mega Byte |
| MCAS | Microsoft Cloud App Security |
| MD | Člověkoden, pracovní čas jedné osoby odpovídající jednomu pracovnímu dni, tedy typicky 8 hodin (man-day) |
| MDM | Správa mobilních zařízení (Mobile Device Management) |
| MFA | Vícefázové ověření (Multifactor Authentication) |
| On-premise | On-premise software je takový software, který lze instalovat a provozovat v prostorách organizace, která jej využívá |
| OS | Operační Systém |
| OTP | Jednorázové heslo (One Time Password) |
| PAM | Správa privilegovaných přístupů (Privileged Access Management) |
| PD | Pracovní Den |
| PKI | Infrastruktura správy a distribuce veřejných klíčů (Public Key Infrastructure) |
| Privilegovaný účet | Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění |
| RDP | Protokol na přenos vzdálené plochy (Remote Desktop Protocol) |
| SIEM | Systém pro správu bezpečnostních událostí (Security Information and Event Management) |
| SLA | Dohoda o úrovni poskytovaných služeb (Service Level Agreement) |
| SSH | Zabezpečený protokol pro připojení k serverům |
| SSO | Systém jednotného přihlášení (Single Sign-On) |
| Stress skript | Skript nebo funkcionalita, která simuluje zátěž systému, například generuje logy apod. |
| SW | Software |
| SŽ | Správa železnic, státní organizace |
| UAS | Uživatelsko-aplikační síť |
| Uchazeč | Subjekt, který se v rámci tohoto zadávacího řízení uchází o dodávku řešení Centrálního Log Managementu. Uchazeč, který bude vybrán SŽ, se stane dodavatelem |
| Uživatel CLM | Uživatel CLM je administrátor (interní či externí), který používá CLM řešení pro přístup k záznamům/logům ze spravovaných koncových systémů.  Uživatel CLM je také administrátor CLM, který provádí dohled na správný běh CLM a správu jeho konfigurací |

Seznam zkratek pro specifické aplikace SŽ:

|  |  |
| --- | --- |
| Zkratka | Popis |
| ASVC | Automatické stavění vlakových cest |
| DŘT | Dispečerská řídicí technika |
| ČD-IS | České dráhy informační systém? |
| DDTS | Dálková diagnostika technologických systémů |
| CDP | Centrální dispečerské pracoviště |
| CDS | Centrální dispečerský systém |
| DŽDC | Dispečer železniční dopravní cesty |
| DŽIN | Dispečer železniční infrastruktury |
| ED | Elektro dispečer |
| GVD | Grafikon vlakové dopravy |
| SSZT | Správa sdělovací a zabezpečovací techniky |
| ST | Správa tratí |
| SŽE | Správa železniční energetiky |
| TDS | Technologický a dohledový systém |
| TECHLAN | Technologická datová síť |
| TLS | Technologický systém železniční dopravní cesty |
| TDCDP | Traťový dispečer dálkového ovládání zabezpečovacího zařízení na CDP |
| VPN | Virtuální privátní síť (Virtual Private Network) |
| VS | Vlakové soupravy |
| ŽDC | Železniční dopravní cesta |
| ZZ | Zabezpečovací zařízení |

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávacího řízení pro výběr dodavatele Centrálního Log Managementu (dále jen “CLM“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“). Dokument popisuje technické a jiné požadavky na nový CLM. Dále popisuje současný stav prostředí významné pro vznik nového CLM.

## Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je realizace CLM pro SŽ. Tento CLM zajistí sběr, zpracování, dlouhodobé zaručené ukládání, umožní analyzovat a dlouhodobě ukládat záznamy o událostech v komponentách, systémech a aplikacích SŽ tak, aby byly prokazatelné, chráněné a udržované v souladu se zákonnými a dalšími vyjmenovanými požadavky.

Detekce kybernetických bezpečnostních událostí a vyhodnocování kybernetických bezpečnostních událostí není předmětem této veřejné zakázky.

Tato zakázka bude obsahovat následující poptávané oblasti:

* Analýza
  + Analýza současného stavu a vytvoření konceptu CLM (podrobněji viz. kapitola 6.1)
* Technický návrh (podrobněji viz. kapitola 6.2)
  + Návrh architektury CLM - Vybraný dodavatel na základě analýzy vypracuje Technický návrh implementace v rozsahu a detailu LLD
  + Definice procesů a procedur souviseních s řízením CLM
* Dodávka komponent CLM a jejich integrace do prostředí SŽ
  + Dodávka hardware, software a licencí (podrobněji viz. kapitola 6.3)
  + Zajištění produkčního i testovacího prostředí CLM (podrobněji viz. kapitoly 6.4 a 6.5)
  + Konfigurace a připojení zdrojů logů CLM (podrobněji viz. kapitola 6.6)
  + Provedení testů architektonických, funkčních, bezpečnostních a ostatních požadavků CLM (podrobněji viz. kapitola 6.7)
  + Zajištění pilotního provozu CLM, jeho vyhodnocení a realizace případných nápravných opatření (podrobněji viz. kapitola 6.8)
* Servisní podpora
  + Provedení školení obsluhy CLM (podrobněji viz. kapitoly 6.9 a 6.10)
  + Předání CLM do produkčního užívání (podrobněji viz. kapitola 6.11)
  + Poskytnutí technické podpory provozu CLM (podrobněji viz. kapitoly 6.12 a 6.13)

Způsob realizace CLM musí zajistit mimo jiné soulad s požadavky §22 Vyhlášky č. 82/2018 Sb. - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů – a jeho prováděcích předpisů.

Detailní popis výše uvedených požadavků CLM je uveden v následujících kapitolách tohoto dokumentu.

# Současný stav a popis prostředí

IT aktiva (dále jen “aktiva”) určená pro napojení na CLM jsou geograficky rozprostřena po celém území České republiky a rozdělena do následujících skupin:

1. [Specifické aplikace SŽ](#_Specifické__)
2. [Generické systémy a aplikace](#_Generické_systémy_a) - operační systémy, databáze, virtuální instance, aktivní prvky a další
3. [Bezpečnostní technologie](#_Bezpečnostní_technologie) - systémy zařazené jako bezpečnostní prvky v rámci infrastruktury SŽ

S ohledem na citlivost informací detailně popisujících Specifické aplikace SŽ a jejich geografické umístění, budou tyto informace dostupné Uchazeči pouze na základě podepsané dohody o mlčenlivosti jejíž vzor je v Příloze č. 9 Zadávací dokumentace

## Souhrnné objemy logů

Výpočet odhadu objemu logů a EPS, který bude zpracovávat CLM, vychází z informací dostupných v době zveřejnění tohoto dokumentu. Dále u aktiv, pro která nejsou žádné informace o objemu logů k dispozici, odhad souhrnného objemu vychází z předpokladu 70% vytíženosti maximální kapacity aktiva. Pro některá aktiva byl zvolen prostý odhad dle velikosti SŽ.

Uvedené objemy a informace jsou dynamického charakteru a při změně logovací strategie může dojít k jejich změně.

V rámci analýzy provedené vybraným dodavatelem mohou být poskytnuty informace z provozního monitoringu a data zatížení jednotlivých aktiv pro provedení vlastního odhadu velikosti a typu logů – zejména pro aktiva, která v následujících kapitolách nemají uvedený objem logů nebo další informace.

Pro každou skupinu aktiv je specifikována podmnožina aktiv podle seznamu primárních a podpůrných aktiv, která tvoří kritickou informační infrastrukturu a musí být tedy řízena podle § 22, vyhlášky č.82/2018 a požadavků definovaných v [Kapitole 5.6 Požadavky dle § 22 vyhlášky č. 82/2018](#_Požadavků_dle_§).

|  |  |  |  |
| --- | --- | --- | --- |
| Skupina | Objem dat za 24 hodin | Z toho podíl kritické informační infrastruktury | EPS |
| Specifické aplikace SŽ | 800 GB | 25 % | 20 000 |
| Generické systémy a aplikace | 17 TB | 25 % | 100 000 |
| Bezpečnostní technologie | 2 TB | 30 % | 15 000 |
| **Celkem** | **19,8 TB** | **5,05 TB** | **135 000** |

## Specifické aplikace SŽ

Přehled specifických aplikací SŽ, včetně formátu a odhadu objemu sbíraných logů podle metodiky uvedené v [Kapitole 4.1. Souhrnné objemy logů](#_Souhrnné_objemy_logů).

Přehled specifických aplikací SŽ:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Typ | Název aplikace | Objemu logů za den [MB] | Formát |
| 1 | Specifické aplikace SŽ | DŘT | 4 514 | log, csv |
| 2 | Specifické aplikace SŽ | DDTS | - | n/a |
| 3 | Specifické aplikace SŽ | ISOŘ | 1,04 | SQL DB, txt |
| 4 | Specifické aplikace SŽ | ISOŘ RDV | 0,44 | SQL DB, txt |
| 5 | Specifické aplikace SŽ | EDD | 124 275 | log |
| 6 | Specifické aplikace SŽ | GTN (celkem 650 instancí) | 200 000 | log |
| 7 | Specifické aplikace SŽ | ROSA I | 43 571 | txt |
| 8 | Specifické aplikace SŽ | Portál provozování dráhy | 14,4 | adresářová struktura, události v samostatných souborech log |
| 9 | Specifické aplikace SŽ | KADR | - | SQL, DB, txt |
| 10 | Specifické aplikace SŽ | GRADO (celkem až 150 instancí) | 1 400 | html, log |
| 11 | Specifické aplikace SŽ | ComposT | - | syslog, DB logy Oracle, txt formát apl. logu |
| 12 | Specifické aplikace SŽ | Rozkazy | 2 028 | log, členěno podle zdroje, systémové logy Windows, txt |
| 13 | Specifické aplikace SŽ | SAP ERP (R/3, do budoucna S/4) | - | - |
| 14 | Specifické aplikace SŽ | Spisová služba (ERMS) | - | - |
| 15 | Specifické aplikace SŽ | Dodavatelé, odběratelé – žádanky systém | - | - |
| 16 | Specifické aplikace SŽ | IS C.E.Sta | - | - |
| 17 | Specifické aplikace SŽ | ISPD | - | - |
| 18 | Specifické aplikace SŽ | Provozní stav sítě tratí (PSST) | - | - |
| 19 | Specifické aplikace SŽ | Hybridní model zúčtování TEE | - | - |
| 20 | Specifické aplikace SŽ | DCS (Data Collection System) - sběr dat z elektroměrů lokomotiv | - | - |
| 21 | Specifické aplikace SŽ | Zákaznický portál Energie | - | - |
| 22 | Specifické aplikace SŽ | KAC (Kontrolně-analytické centrum) | - | - |
| 23 | Specifické aplikace SŽ | Centrální rozkazy | - | - |
| 24 | Specifické aplikace SŽ | CI Common interface | - | - |
| 25 | Specifické aplikace SŽ | CSV | - | - |
| 26 | Specifické aplikace SŽ | Datový sklad SŽDC | - | - |
| 27 | Specifické aplikace SŽ | DOMIN (TSI databáze omezení infrastruktury) | - | - |
| 28 | Specifické aplikace SŽ | ETD – Electronic Timetable Display | - | - |
| 29 | Specifické aplikace SŽ | EZOP – Elektronický zobrazovací panel | - | - |
| 30 | Specifické aplikace SŽ | IS MIMOZA | - | txt |
| 31 | Specifické aplikace SŽ | KANGO-IS komplexní sestava jízdního řádu | 0,5 | - |
| 32 | Specifické aplikace SŽ | KAPO | 120 | txt |
| 33 | Specifické aplikace SŽ | REVOZ (Registr vozidel) | 20 | txt |
| 34 | Specifické aplikace SŽ | VITAMIN | 100 | txt |
| 35 | Specifické aplikace SŽ | RNE TIS (Europtirails) | - | - |
| 36 | Specifické aplikace SŽ | KISKAN SŽDC | - | - |
| 37 | Specifické aplikace SŽ | MIMOZA PŘEKÁŽKY aplikační server | 5 | txt |
| 38 | Specifické aplikace SŽ | MIMOZA PŘEKÁŽKY klient | 0,25 | txt |
| 39 | Specifické aplikace SŽ | MIMOZA PŘEKÁŽKY importní modul | 120 | txt |

## Generické systémy a aplikace

Přehled generických systémů a aplikací, včetně typu logu a odhadu objemu sbíraných logů, a počtu instancí systémů podle metodiky uvedené v [Kapitole 4.1. Souhrnné objemy logů](#_Souhrnné_objemy_logů).

Generické systémy a aplikace jsou rozděleny na:

#### Doménové řadiče, operační systémy, služby

1. Síťové technologie

### Doménové řadiče, operační systémy, služby

| ID | Typ | Koncový systém | Počet prvků / instancí | Poznámka |
| --- | --- | --- | --- | --- |
| 1 | Active Directory | doména UADF | 1 | Odhad Logů v MB za den:4  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 2 | Active Directory | doména UADF | 1 | Odhad Logů v MB za den:240  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 3 | Active Directory | doména UADF | 1 | Odhad Logů v MB za den:21  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 4 | Active Directory | doména UADFD01 | 1 | Odhad Logů v MB za den:4  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 5 | Active Directory | doména UADFD01 | 1 | Odhad Logů v MB za den:15 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 6 | Active Directory | doména UADFD01 | 1 | Odhad Logů v MB za den:280  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 7 | Active Directory | doména UADFD02 | 1 | Odhad Logů v MB za den:5  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 8 | Active Directory | doména UADFD02 | 1 | Odhad Logů v MB za den:30 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 9 | Active Directory | doména UADFD02 | 1 | Odhad Logů v MB za den:25  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 10 | Active Directory | doména MADF | 1 | Odhad Logů v MB za den:2 000  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 4 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 11 | Active Directory | doména MADF | 1 | Odhad Logů v MB za den:37 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 4 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 12 | Active Directory | doména MADF | 1 | Odhad Logů v MB za den:4 000  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 4 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 13 | Active Directory | doména OADF | 1 | Odhad Logů v MB za den:1 500  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 14 | Active Directory | doména OADF | 1 | Odhad Logů v MB za den:2 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 15 | Active Directory | doména OADF | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 16 | Active Directory | doména EADF | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 17 | Active Directory | doména EADF | 1 | Odhad Logů v MB za den:5 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 18 | Active Directory | doména EADF | 1 | Odhad Logů v MB za den:20  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale doménu tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 19 | Server | MS Exchange  CAS server | 1 | Odhad Logů v MB za den:250  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale systém tvoří 6 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 20 | Server | MS Exchange  CAS server | 1 | Odhad Logů v MB za den:40 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 6 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 21 | Server | MS Exchange  CAS server | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale systém tvoří 6 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 22 | Server | MS Exchange  Content servery | 1 | Odhad Logů v MB za den:1 500  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale systém tvoří 15 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 23 | Server | MS Exchange  Content servery | 1 | Odhad Logů v MB za den:80 000  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 15 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 24 | Server | MS Exchange  Content servery | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale systém tvoří 15 serverů. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 25 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:20  Typ Logu: Windows Log  Application log  V budoucnu budou službu zajišťovat 4 servery, služba je využívána ve VELICE omezené míře, v budoucnu dojde k výraznému navýšení využití. |
| 26 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:150  Typ Logu: Windows Log  Security log  V budoucnu budou službu zajišťovat 4 servery, služba je využívána ve VELICE omezené míře, v budoucnu dojde k výraznému navýšení využití. |
| 27 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:50  Typ Logu: Windows Log  System log  V budoucnu budou službu zajišťovat 4 servery, služba je využívána ve VELICE omezené míře, v budoucnu dojde k výraznému navýšení využití. |
| 28 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 29 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 30 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 31 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Application log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 32 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 33 | Služba | Doménový řadič | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 34 | APP | PROXY | 1 | Odhad Logů v MB za den:200  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 35 | APP | PROXY | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  System log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 36 | APP | PROXY | 1 | Odhad Logů v MB za den:10  Typ Logu: Windows Log  Security log  Hodnoty za jeden server, ale systém tvoří 2 servery. Je tedy potřeba uvažovat o násobku objemu dat logů. |
| 37 | APP | PROXY | 1 | Typ Logu: w3c file  Odhad Logů v MB za den:50 000  Provozní proxy logy – logování jednotlivých přístupů  Logy jsou zálohovány a ručně a uchovány pro případné analýzy mimo server. |
| 38 | APP | Doménový řadič | 1 | Odhad Logů v MB za den:60  typ Logu Windows Log  Suma za všechny generované logy. |
| 39 | APP | Doménový řadič | 1 | Odhad Logů v MB za den:60  typ Logu Windows Log  Suma za všechny generované logy. |
| 40 | OS | Doménový řadič | 1 | Odhad Logů v MB za den:11 404 800  Suma za všechny generované logy. |
| 41 | DB | Oracle databáze | - | - |

### Síťové technologie

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| ID | Typ | Typová řada | Páteř | Počet | Pozn. |
| 1 | DWDM páteřní boxy + repeatery | Cisco ONS 15454 | ANO | 22 |  |
| 2 | SDH páteřní boxy Cisco ONS | Cisco ONS 15454 | ANO | 30 |  |
| 3 | SDH páteřní boxy Nortel | OME 6150 | ANO | 2 |  |
| 4 | SDH páteřní boxy Ericsson | SPO 1460 | ANO | 14 |  |
| 5 | SDH přístupové boxy Cisco ONS | Cisco ONS 15305 | NE | 549 |  |
| 6 | SDH přístupové boxy Ericsson | SPO 1460 | NE | 122 |  |
| 7 | SDH přístupové boxy Alcatel | Alcatel-Lucent 1646 | NE | 57 |  |
| 8 | Páteřní datové uzly INTRANET (UAS) | Cisco C 3xxx, C 7xxx, ISR 2xxx, ISR 3xxx, ASR 9xx, ASR 1xxx, | ANO | 50 |  |
| 9 | Páteřní datové uzly technologické | Cisco ISR 2800, ASR 900 | ANO | 7 |  |
| 10 | Přístupové datové uzly technologické | Cisco ISR 2xxx, 4xxx, 8xx, 9xx | NE | 6 |  |
| 11 | Přístupové datové uzly INTRANET (UAS) | Cisco C2xxx, C3xxx, ISR všech řad | NE | 187 |  |
| 12 | Páteřní datové uzly MPLS P | Cisco ASR 9000, ASR 100 | ANO | 4 |  |
| 13 | Páteřní datové uzly MPLS CE | Cisco ASR 900 | ANO | 3 |  |
| 14 | Přístupové datové uzly MPLS PE Cisco | Cisco ASR 900, ASR 9000 | ANO | 93 |  |
| 15 | Přístupové datové uzly MPLS PE NOKIA | 7705 - SAR | NE | 24 |  |
| 16 | VoIP gateways | Cisco C 3700, ISR 2xxx, 4xxx | NE | 187 |  |
| 17 | Switche páteř INTRANET (UAS) | C 29xx, C3xxx, C4000, C6xxx, C9xxx | ANO | 39 |  |
| 18 | Switche páteř v technologických sítích | C3xxx | ANO | 2 |  |
| 19 | Switche L3 INTRANET (UAS) | C3xxx, C9xxx | NE | 95 |  |
| 20 | Switche L2 INTRANET (UAS) | typicky C2950, 2960 C9200 | NE | 2 810 | Malé procento "non Cisco" switchů, např. HP, Zyxel a další |
| 21 | Switche L3 TECHLAN | C3xxx, C4000, C9xxx | NE | 178 |  |
| 22 | Switche L2 TECHLAN | C29xx, C3xxx, C92xx | NE | 2 210 |  |
| 23 | WiFi controllery | AIR CT25xx, C98xx | ANO | 16 |  |
| 24 | WiFi AP (řízené controllerem) | AIR AP18xx, IW37xx, C9105 | NE | 377 |  |
| 25 | WiFi AP (autonomní) | Ubiquiti, TRENDnet | NE | 6 |  |
| 26 | Firewally | ASA, FPW, Fortigate | NE | 41 |  |

## Bezpečnostní technologie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | Typ | Název | Objemu logů za den [MB] | Formát |
| 1 | Bezpečnostní technologie | Logserver (ČD-IS) | - | - |
| 2 | Bezpečnostní technologie | Azure AD Connect | - | - |
| 3 | Bezpečnostní technologie | Azure AD | - | - |
| 4 | Bezpečnostní technologie | Vícefaktorové autentizace | - | - |
| 5 | Bezpečnostní technologie | PKI | - | - |
| 6 | Bezpečnostní technologie | MFA | - | - |
| 7 | Bezpečnostní technologie | CA | - | - |
| 8 | Bezpečnostní technologie | MDM | - | - |
| 9 | Bezpečnostní technologie | Compliance Management | - | - |
| 10 | Bezpečnostní technologie | MCAS | - | - |
| 11 | Bezpečnostní technologie | ATP/ATI | - | - |
| 12 | Bezpečnostní technologie | Bitlocker | - | - |
| 13 | Bezpečnostní technologie | Časové servery | - | - |
| 14 | Bezpečnostní technologie | Antivirové řešení | - | - |
| 15 | Bezpečnostní technologie | PAM | - | - |
| 16 | Bezpečnostní technologie | IDM | - | - |
| 17 | Bezpečnostní technologie | Tacacs+ | - | - |
| 18 | Bezpečnostní technologie | Radius | - | - |

# Požadavky CLM

## Funkční požadavky

| ID | Název požadavku | Popis požadavku |
| --- | --- | --- |
| F1 | Škálovatelnost prostředí | * Navrhované řešení musí splňovat všechna kritéria pro budoucí rozšíření systému a škálovatelnost o další:  1. Zdrojové systémy 2. Funkční logování 3. Operace s logy 4. Filtrování 5. Šablony 6. Hardware  * Navržená architektura prostředí musí umožnovat škálování a zvětšování v rámci použitého HW a SW. * Škálovatelnost celého systému musí být do budoucna schopná akceptovat až pětinásobný objem stávajících logů |
| F2 | Dlouhodobé uložení logů | Systém musí umožnovat funkcionalitu dlouhodobého uložení logů (logy, které se nebudou dále zpracovávat) dle následujících požadavků:   * Dlouhodobě uložené logy musí být uloženy odděleně od CLM úložiště * Úložiště (HW i SW) dlouhodobě ukládaných logů je součástí dodávky budoucího dodavatele * Délka uschování všech logů mimo logů primárných a podpůrných aktiv SŽ v dlouhodobě ukládacím režimu: 12 měsíců * Délka uschování logů primárných a podpůrných aktiv SŽ v dlouhodobě ukládacím režimu: 18 měsíců a v souladu s požadavky § 22, vyhlášky č.82/2018 * CLM systém musí být schopen provádět dlouhodobé ukládání na externím uložišti a mít možnost připojit se na externí uložiště (dlouhodobé úložiště uložiště třetích stran) |
| F3 | Požadavky na funkcionality zpracování logů | * Minimální délka uchování aktuálních logů s možností zpracování: 30 dnů * Možnost provádění kombinovaných forenzních vyhledávacích možností v uživatelské konzoli s možností nastavení minimálně následujících parametrů:  1. Zdroj logu (s možností vlastního pojmenování zdroje nebo skupiny zdrojů) 2. Čas vzniku události 3. Čas přijetí logu 4. Kombinace vyhledání s možností podmiňování IF (tj. na základě jedné události v “systému A“ a současně v případě vzniku další události v „systému B“ vygeneruj akci – e-mail, upozornění, apod.) 5. Automatizované a plánované aktivity v podobě výše popsaného požadavku 6. Možnost vytvoření aktivit na základě nálezu vyhledávaného řetězce 7. vyhledávání musí umožnit hledat kromě zadaných hodnot také s uvedením “wildcards” nebo regulárních výrazů, a to pro všechny podporované atributy (nejen pro vyjmenované)  * Sběr a ukládání nestrukturovaných logů všech datových typů * Logy se musí ukládat v původním stavu a nesmí být umožněno jejich editování * Možnost indexace logů * Možnost automatizace zpracování s pomocí skriptů * Možnost vizualizace s přednastavenými šablonami * Možnost normalizace a standardizace dle přednastavených šablon * Možnost autorizačních oprávnění na úrovni zdroje logů * Možnost provádět log enrichment na základě aktivit jiných logů a zdrojů * Logování v reálném čase s maximálním zpožděním nižším než 5 sekund * Možnost vyhledání a seskupení logových sestav na základě externího zdroje, například stažených šablon * Možnost zpracování událostí (událost je jeden či více záznamů logicky spojených a zároveň provedených ve stejný časový okamžik) * Možnost zpracování více událostí korelovaných přes identifikátor |
| F4 | Zabezpečení prostředí | * CLM řešení musí používat šifrované uložiště. Musí být použit takový kryptografický algoritmus, který odpovídá požadavkům NÚKIB v dokumentu MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY * CLM řešení musí používat autentizační a autorizační mechanismy založené na Centrálním IDM systému implementovaném v SŽ   CLM řešení musí mít možnost lokálního zakládání a využívání účtů pro případ nedostupností autentizačních služeb centrálního IDM   * CLM řešení musí mít možnost oddělení prostředí pro jednotlivé instance systémů * CLM řešení musí mít Administrátorskou konzoli s možností administrace všech komponent, služeb a nastavení * Všechny komponenty CLM řešení musí splňovat požadavky kybernetické bezpečnosti v podobě hardeningu systémů. Budoucí Dodavatel musí doložit jaký způsob hardeningu je použit * CLM řešení musí umožnovat přidělení oprávnění pro uživatele na úroveň typu logu a zdroje logu. * Aktivity všech uživatelů log managementu v rámci SŽ se musí logovat minimálně v tomto rozsahu a současně tak, aby byl splněn požadavek § 22 vyhlášky č. 82/2018:  1. Přihlášení 2. Neúspěšný pokus o přihlášení 3. Odhlášení 4. Úpravy v systému 5. Pokus o neautorizovanou úpravu 6. Smazání údajů 7. Úpravy prav uživatelů 8. Smazání uživatele 9. Přístup do lokálního uložiště logů 10. Přihlášení pod administrátorským účtem 11. Pokus o neautorizovanou změnu  * Funkcionalita pro udělení časového razítka a digitálního podpisu logů musí být realizována prostřednictvím interní certifikační autority. * CLM řešení musí umožnovat automatické anonymizace datových sestav, logů a událostí na základě přednastaveného algoritmu/příkazu. * Před předáním do provozu na všech komponentách systému musí být proveden hardening všech jednotlivých komponent CLM dle CIS Benchmarku poslední aktualizace pro každou komponentu. (Pro komponenty, pro které neexistuje CIS benchmark, musí být prokázán hardening systémů ekvivalentním způsobem.) Součástí předávky do provozu jsou i všechny testy uvedené v kapitole [Testování](#_Testování). * Všechny datové toky musí být šifrované a současně takto musí být zabezpečena i citlivá komunikace mezi komponentami, s externími systémy nebo s uživateli. Musí být použit takový algoritmus, který odpovídá požadavkům NÚKIB v dokumentu MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY |
| F5 | Cloudové Logy | * Navrhované řešení musí být schopno jako zdroj logů napojit cloudové technologie a systémy v rámci budoucí rozšiřitelnosti a škálovatelnosti. * Navrhované řešení musí umět logovat jakékoliv aplikace nebo operační systémy realizované v těchto cloudových prostředích:  1. Microsoft Azure 2. Google 3. AWS 4. SAP  * Navrhované řešení musí mít základní šablony pro logování výše uvedených cloudových prostředí. |
| F6 | Testovací prostředí | * V rámci dodávky CLM řešení musí být vybudované testovací prostředí. Vývojové/testovací prostředí bude sloužit k testování aktualizací a nových verzí systémů dodaných výrobcem. Zároveň v něm bude probíhat vývoj a testování funkcionalit v rámci rozšiřování zdrojových systémů * Testovací/vývojové prostředí musí zajistit všechny požadované funkční parametry jako prostředí produkční a musí obsahovat minimálně po jedné z komponent použité v produkčním prostředí, aby tak obě prostředí byla identická z pohledu podporovaných funkcí a komponent, a bylo tak možné v testovacím/vývojovém prostředí řádně otestovat veškeré funkcionality a vlastnosti konfigurovatelné v produkčním prostředí. * SŽ požaduje minimálně 20 administrátorských účtů pro testovací prostředí. * Testovací/vývojové prostředí nemusí být nasazeno v režimu vysoké dostupnosti a může být instalováno kompletně ve virtuálním prostředí (i v případě, pokud by Uchazeč navrhl pro produkční prostředí některou z komponent jako fyzický HW). * Všechny změny v rámci řešení (zejména upgrade, bezpečnostní záplaty, nové funkcionality a další nové verze řešení nebo jeho částí) musí být řádně otestovány Uchazečem ještě před nasazením do produkčního prostředí SŽ. V rámci implementace řešení lze produkční prostředí považovat za testovací až do fáze akceptačních testů. |

## Architektura řešení

| ID | Název požadavku | Popis požadavku |
| --- | --- | --- |
| A1 | Technologie CLM | * Architektura CLM řešení musí obsahovat minimálně následující logické komponenty:  1. Kolektor 2. Aplikační server / službu pro zpracování Logů/Engine 3. Centrální uložiště 4. Load Balancer 5. Buffer 6. Dashboard 7. Konzoli/Modul pro nahlížení Logů, tj. prezentační vrstvu 8. Administrační konzoli 9. Konzoli pro tvorbu pravidel, filtru a vyhledávání 10. Dlouhodobé uložiště |
| A2 | Využití cloud řešení | * Je požadováno on-premise řešení |
| A3 | Použití agentů | * Požadované řešení je bezagentní. |
| A4 | Komponenty | * Uchazeč musí navrhnout vhodné umístění všech komponentů jím navrženého řešení dle síťové architektury SŽ. * SŽ předpokládá využití virtualizace, pokud Uchazeč nespecifikuje nutnost použití dedikovaného HW. * Síť SŽ je routována tak, aby připojované systémy byly dostupné z kterékoliv lokality. * Aktuální síťové technologie jsou uvedeny v Příloze č. 2. Zadávací dokumentace. |
| A5 | Load Balancer | * Vzhledem ke zpracování velkého počtu logů architektura musí obsahovat Load Balancer. |
| A6 | Filtering | * Navržená architektura musí obsahovat možnost/funkcionalitu pro filtrování logů. |
| A7 | Collecting | * Navržená architektura musí obsahovat potřebné množství kolektorů, pro zpracování všech logů v reálném čase. |
| A8 | Dashboard | * Navržená architektura musí obsahovat komponentu uživatelského dashboardu s možnostmi vizualizace a personalizace dostupných logových sestav, s možností tvorby reportů, jejích exportů do jiných formátů, apod. |
| A9 | Dlouhodobé úložiště | * Navržená architektura musí obsahovat návrh dlouhodobého úložiště pro uschování logů v časové ose uvedené ve funkčních požadavcích. * Architektura musí umět rozlišit logy a typ jejích uložiště, ke kterým musí být přístup v reálném čase a k logům dlouhodobě uloženým. |
| A10 | Redundance nodů | * Navržená architektura musí obsahovat HA a redundantní nody, nejlépe v podobě geografického clusteru. * Navržená architektura musí splňovat požadované parametry dle servisního modelu uvedeného v kapitole [Zajištění technické podpory provozu](#_Zajištění_technické_podpory) tak, aby byl dodržen požadavek na SLA za jakýchkoliv okolností. |
| A11 | Buffering | * Navržená architektura musí obsahovat buffer pro průtok logů a jejích udržení ve frontě v minimální délce 6 hodin, pro případ přetížení nebo nedostupnosti (údržby) backendových systémů. |
| A12 | Reálný čas | * Sběr a vyhodnocení přijatých logů musí probíhat v reálném čase s maximálním zpožděním 5 sekund. |

## SW a HW

| **ID** | **Název požadavku** | **Popis požadavku** |
| --- | --- | --- |
| H1 | Využití virtualizace | * CLM řešení je preferováno ve virtuální podobě. Uchazeč musí v nabídce specifikovat:   + Přesné vyčíslení dopadů na zdrojové servery při použití agentů, tj. vyčíslení performance, diskové zátěže a jiných omezení stávající kapacity   + Počet požadovaných virtuálních serverů a fyzických serverů a jejich parametrů s ohledem na dostatečnou výkonnost řešení a současnou adekvátnost parametrů   + Požadavky na parametry komunikačních tras a síťových prostupů mezi jednotlivými komponentami řešení   + Konektivita a konfigurace komunikačních sítí podle podaného technického návrhu zajistí SŽ * V případě, že Uchazečem navržené řešení obsahuje některou komponentu na fyzickém HW, Uchazeč musí v nabídce popsat důvod užití. * Virtualizace je možná pouze na úrovni centrálního HA řešení. * Pro virtualizaci musí být použita platforma VMWare v poslední verzi * V případě využití virtualizace musí Uchazeč v nabídce specifikovat také cenu za HW a SW také pro použitou virtualizační platformu. Tato cena je součástí nabídky Uchazeče. |
| H2 | Velikost úložiště pro dlouhodobé ukládání | * Součástí dodávky CLM musí být návrh úložiště pro dlouhodobé uložení logů. Uchazeč musí v nabídce specifikovat potřebnou kapacitu, typ úložiště a připojení. |
| H3 | HW a SW jako součást dodávky | * Veškerý hardware bude součásti dodávky a bude naceněn v nabídce v rámci projektu implementace CLM. |
| H4 | Popis a Lokalita HW a SW | * Veškerý HW a SW, který bude součást dodávky bude popsán v položkovém seznamu obsahující povinné atributy:   + Označení   + Název komponenty (produktu)   + Role komponenty v systému   + Popis umístění komponenty (včetně geografické lokalizace)   + Technická specifikace produktu   + Množství   + Cena |
| H5 | Technologie pro virtualizace | * Virtualizace prostředí je realizovaná technologií VMWare nebo Hyper-V |
| H6 | Technologie pro servery | * Servery jsou realizované na OS Windows Server nebo na OS Linux jedné z distribucí SuSe, CentOS, RedHat |
| H7 | Technologie pro databáze | * Databáze jsou realizované technologií Oracle DB nebo MS SQL nebo MySQL |
| H8 | Technologie pro aplikační servery | * Platforma aplikačních serverů je realizovaná technologií Oracle WebLogic nebo JBoss |

## Zajištění vysoké dostupnosti

| ID | Název požadavku | Popis požadavku |
| --- | --- | --- |
| D1 | Vysoká dostupnost CLM | * Produkční prostředí CLM musí být instalováno v režimu HA. Musí být zajištěno, aby při výpadku jedné části systému nebyla dotčena funkčnost celého řešení. * Každá z komponent CLM, která je nezbytná pro provoz CLM, musí obsahovat minimálně dvě samostatné instance provozované v HA režimu s maximální dobou přepnutí v řádu jednotek sekund. * Řešení vysoké dostupnosti musí být automatické. Řešení, která vyžadují jakoukoliv manuální intervenci pro přepnutí mezi instancemi v případě vzniku chybového stavu, nejsou přípustná. |

## Integrace

| ID | Název požadavku | Popis požadavku |
| --- | --- | --- |
| I1 | Integrace s IDM řešením | * Součástí dodávky musí být integrace CLM řešení se systémem Centrálního ověřování (IDM). * SŽ požaduje dodávku přesné specifikace REST API na straně CLM řešení, které bude IDM využívat. |
| I2 | Lokálně vytvořené účty | * CLM řešení musí umožnovat vytvářet i lokálně privilegované účty, tj. účty, které nejsou spravovány pomocí IDM systému. |
| I3 | Integrace se helpdesk systémem | * CLM řešení musí být schopné integrace s ITSM (helpdesk) systémem. * CLM řešení musí být schopné integrace s Zabbix systémem * CLM řešení musí být schopné integrace s Active Directory systémem * CLM řešení musí být schopné jak manuálně, tak i automaticky založit servisní požadavek (ticket). * CLM řešení musí být schopné automaticky založit servisní požadavek (ticket) s možností úpravy ticketu automatickým pravidlem. * CLM řešení musí být možné do budoucna integrovat se CMDB tak, aby bylo možné ze CMDB databáze získávat data. |

## Požadavky dle § 22 vyhlášky č. 82/2018

V rámci Centrálního Log Managementu a jeho funkčních, bezpečnostních a ostatních požadavků musí být splněny funkcionality bezpečnostního logování tak, aby v přiměřené míře a za přiměřených nákladů a v rámci řádného hospodaření s náklady, bylo možné dodržet všechny požadavky uvedené v § 22, vyhlášky č. 82/2018.

|  |  |  |
| --- | --- | --- |
| ID | Požadavek | Požadavky na realizaci v rámci organizace Správa železnic |
| S1 | Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů | * CLM musí splňovat možnost zaznamenávat události informačních a komunikačních systémů bez ohledu na jejich způsob sběru, různorodost nebo technickou komplikovanost. * Současně musí mít možnost zaznamenávat všechny uživatelské události. * CLM musí mít možnost zaznamenávat výše zmíněné události kritické infrastruktury pro:  1. Specifické aplikace Správy železnic 2. Generické infrastrukturní páteřní a kritické systémy (myšleno nespecifické standardní a univerzální systémy z platforem Microsoft, Linux, Unix apod.) 3. Bezpečnostní technologie jako firewally, sondy apod., aktivní a jiné instance použité v rámci architektury kybernetické bezpečnosti |
| S2 | Záznam bezpečnostních a provozních událostí | * Uchazeč musí v rámci nabídky a implementace CLM dodat takové řešení, které bude schopné zaznamenávat události kritických aktiv informačního a komunikačního systému. * V rámci organizace SŽ se jedná o páteřní a kritické infrastrukturní a specifické systémy, které budou posílat události do CLM. * Všechny bezpečnostně provozní informace/události musí být zaznamenány, tj. minimálně v rozsahu událostí, které mohou způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací. * Budoucí Dodavatel navrhne a naimplementuje systém, který umožní zaznamenávat všechny zdrojové informace v systémech Správy železnic v RAW podobě (neměnitelná podoba logů, tak, jak byla vytvořena původním zdrojem). |
| S3 | Aktualizace rozsahu IT aktiv | * CLM musí mít možnost pružně reagovat na stávající aktiva a na aktiva, která do budoucna na základě rozhodnutí povinné osoby přibydou do kritické infrastruktury a systémů. Funkcionalita auto discovery (funkce pro zjišťování nových zdrojů logů) není požadována. |
| S4 | Jednoznačná síťovou identifikaci zařízení původce | * CLM musí mít jednoznačnou a konkrétní možnost na základě defaultní funkcionality zajistit jednoznačnou původní identifikaci zdroje logů i v případě, že po cestě do CLM byla změněna (dále musí mít možnost zobrazit RAW Log v původní nezměněné podobě). |
| S5 | Identifikace data a času | * CLM řešení umožní zaznamenávat datum a čas událostí tak, aby byl záznam unikátní bez ohledu na zdrojové systémy a jejích různorodost, současně bude zpětně identifikovatelný pro daný zdroj a čas. * Časová synchronizace musí probíhat s časovými servery SŽ. |
| S6 | Identifikace typu činnosti | * CLM řešení musí být schopné logovat typ činnosti, například spuštěné služby nebo jiné činnosti, které budou vznikat na základě několika kritérií výskytu logů. |
| S7 | Identifikace původce činnosti | * CLM řešení musí poskytnout informaci o identifikaci zdrojového technického aktiva (systém, zařízení apod.). * CLM řešení musí zaznamenávat a ukládat informaci o identifikaci zdrojového technického aktiva (systém, zařízení apod.). * V případě implementace u SŽ musí mít každý log konkrétně uvedený zdroj (který bude možné pojmenovat dalším názvem). |
| S8 | Identifikace identity původce činnosti | * CLM řešení musí být schopné zajistit zobrazení identifikace účtu, který bude unikátní/poskytnutý systémem a ve kterém byla provedena změna. * CLM řešení musí být schopno zaznamenávat identifikaci účtu, který bude unikátní/poskytnutý systémem a ve kterém byla provedena změna. |
| S9 | Identifikace zařízení původce činnosti | * V případě síťových prvků musí být jasně a konkrétně propsána všechna zdrojová zařízení v rámci prezentace logů v dashboardu nebo libovolném, nejen grafickém zobrazení. |
| S10 | Identifikace úspěšnosti činnosti | * Pokud to zdrojový systém umožnuje, musí být CLM nastaven tak, aby logoval úspěšnou nebo neúspěšnou činnost jakéhokoliv charakteru ve zdrojovém systému a současně toto kritérium musí být jako jedna z možností filtrace. |
| S11 | Zajištění ochrany informací | * CLM systém musí konkrétně jasně a explicitně dodržovat zásady celistvosti, důvěryhodnosti a dostupnosti veškerých sbíraných dat. * CLM systém musí šifrovat veškerý obsah dat. Musí být použit takový kryptografický algoritmus, který odpovídá požadavkům NÚKIB v dokumentu MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY * CLM systém musí mít možnost napojení na (již existující) SSO a dále musí mít možnost použít autorizační mechanismy s možností multifaktorové autorizace. CLM systém musí mít možnost použít kartu s certifikátem pro ověření interního uživatele SŽ. Budoucí Dodavatel nebude implementovat SSO řešení. * V systému CLM musí být použitá interní certifikační autorita pro podepisování logů. * Systém CLM musí umožnovat podepisovat batch (balíček) informací, nikoliv samotné logy. Budoucí Dodavatel navrhne vhodný způsob deklarace a prokázání času v podepsaných balíčcích. * Veškerá komunikace bude zabezpečena prostřednictvím standardních protokolů dle požadavků NÚKIB v dokumentu MINIMÁLNÍ POŽADAVKY NA KRYPTOGRAFICKÉ ALGORITMY |
| S12 | Identifikace přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů | * CLM musí zaznamenávat všechna přihlášení, včetně neúspěšných pokusů do všech systémů označených jako kritická informační infrastruktura. |
| S13 | Identifikace činností provedených administrátory | * CLM musí zaznamenávat veškeré události a aktivity, které byly prováděny administrátory. |
| S14 | Identifikace manipulace s účty, oprávněními a právy | * CLM musí zaznamenávat jakékoliv manipulace s účty, jejích oprávněními a právy. |
| S15 | Identifikace neprovedení činností v důsledku nedostatku přístupových práv a oprávnění | * CLM musí zaznamenávat všechny nedokončené činnosti které vznikly na základě nedostatečných oprávnění, současně tyto události musí být možné filtrovat prostřednictvím předem nastavených filtrů. |
| S16 | Identifikace činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému | * CLM musí umožnovat monitorovat a sbírat veškeré události ohledně činností konkrétních uživatelů a dále tyto logy musí být možné filtrovat na základě kritérií. |
| S17 | Identifikace zahájení a ukončení činností technických aktiv | * CLM musí umožnovat editaci (přidání – odebrání) zdrojových systémů logů tak, aby bylo možné pružně reagovat na zahájení a ukončení činností kritických systémů. |
| S18 | Identifikace kritických i chybových hlášení technických aktiv | * CLM musí umožnovat sbírat kritické a chybové události v rámci kritické infrastruktury a současně tyto události musí být filtrovatelné, tj. musí být nastavena možnost filtrace na základě předem definovaných kritérií. |
| S19 | Identifikace přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí | * CLM musí umožnovat sbírat jakékoliv události vzniklé při pokusech o změnu logů nebo jakoukoliv manipulaci s logy a současně musí umožnovat tyto události alarmovat prostřednictvím e-mailu nebo jiného komunikačního kanálu odpovědným osobám. |
| S20 | Zajištění synchronizace jednotného času technických aktiv nejméně jednou za 24 hodin | * CLM musí umožnovat synchronizaci času minimálně jednou za 24 hodin, a v případě zjištění nesrovnalostí musí umožnovat odeslat alarm prostřednictvím e-mailu nebo jiného komunikačního kanálu. |
| S21 | Dlouhodobé uložení logů | * CLM musí uschovávat veškeré logy v souladu s požadavkem F2 v [kapitole 5.1](#_Funkční_požadavky) * K těmto záznamům musí mít přístup a odpovídá za ně odpovědná osoba – CISO nebo jiná určená osoba. |

### Bezpečnostní monitoring jako součásti CLM

S ohledem na § 22, vyhlášky č. 82/2018 a realizaci CLM v prostředí SŽ, musí navrhnuté řešení být schopné spravovat elementární požadavky z platformy bezpečnostního monitoringu.

|  |  |  |
| --- | --- | --- |
| ID | Požadavek | Požadavky na realizaci v rámci organizace Správa železnic |
| S22 | Dashboard a zobrazení aktuálních událostí za jednotlivý předem nastavený časový úsek | Navrhované řešení musí umět zobrazit události dle nastaveného časového úseku v rámci uživatelského dashboardu. |
| S23 | Alerting | * Navrhované řešení musí umět zasílat upozornění na základě předem nastavených kritérií na specifické adresy jednotlivých uživatelů skrze specifické kanály (e-mail, SMS, hlasová zpráva nebo chat). * Navrhované řešení musí umět komunikovat s dalšími systémy prostřednictvím zasílání zpráv nebo prostřednictvím komunikace API do jiných systémů. |
| S24 | Korelace logů | Základní korelace logů na základě předem stanovených filtrů a kritérií s možností jednoznačné identifikace ohroženého aktiva. |
| S25 | Šablony | Řešení musí umožnovat práci se šablonami a tvorby základních šablon včetně možností zapojení bezpečnostních kritérií. |

## Počet uživatelů CLM

Níže uvedená tabulka uvádí přehled počtu uživatelů, kteří budou přistupovat do systému CLM a dalších parametrů pro stanovení sizingu licencí a HW:

|  |  |
| --- | --- |
| Typ uživatele | Počet uživatelů / Parametr |
| Administrátor | 100 |
| Jmenný uživatel | Maximálně 500 |
| Současně připojení uživatelé v běžném provozu | Maximálně 20 |
| Současně připojení uživatelé ve špičce | Maximálně 40 |
| Průměrná délka uživatelské relace za den | 4 hod |

# Požadavky na dodávku

Definice požadavků na provedení činností v rámci zavedení CLM do prostředí SŽ.

Dodávka se musí skládat alespoň z níže uvedených činností:

1. Vypracování analýzy
2. Definice Technického návrhu implementace
3. Dodávka SW, HW a licencí
4. Dodávka Produkčního a testovacího prostředí
5. Instalace
6. Konfigurace
7. Testování
8. Pilotní provoz
9. Dokumentace
10. Školení
11. Předání do provozu
12. Zajištění technické podpory provozu
13. Nadstandardní služby

SŽ požaduje popis návrhu realizace jednotlivých výše uvedených činností. Tento popis bude součástí nabídky podle šablony v Příloze č. 3 Zadávací dokumentace.

## Analýza

Analýza současného stavu, zpřesnění požadavků a vytvoření konceptu CLM. Vybraný dodavatel provede vlastní analýzu nutnou k tvorbě technického návrhu implementace a k zajištění všech potřeb nutných k plnění požadavků podané nabídky.

Výstupem analýzy bude obecný popis komponent, jejich vztahů, kapacit atd., dále je požadován popis architektury budoucího CLM, popis operačního modelů a procesů dotčených CLM.

Výstup analýzy musí být oboustranně schválen (SŽ i budoucím dodavatelem) před zahájením kroku [Definice technického návrhu implementace](#_Definice_Technického_návrhu). Technický návrh implementace musí vycházet ze schváleného znění výstupu Analýzy a být s ním plně v souladu.

## Definice Technického návrhu implementace

Před zahájením integračních aktivit musí vzniknout dokument Technický návrh implementace obsahující popis technického řešení CLM. Znění tohoto dokumentu musí být oboustranně schválené SŽ i Budoucím Dodavatelem a poté tvoří závazný dokument pro nové CLM řešení.

|  |  |  |
| --- | --- | --- |
| ID | Kapitola | Popis |
| T1 | Úvod | * Popis účelu dokumentu, popis rozsahu, cíle, katalog změn a dopady |
| T2 | LLD specifikace | * Specifikace celé implementace na úrovni LLD, včetně popisu architektury, členění a všech funkčních požadavků uvedených v technické specifikaci SŽ |
| T3 | Business požadavky | * Specifické požadavky business vlastníka na integraci, implementaci a obsah, se současným přihlédnutím k funkčním požadavkům |
| T4 | HW a SW prostředí | * Detailní popis potřebného HW a SW včetně rozpisu všech modulů, aktiv, virtuálních instancí do úrovně virtuálních kontejnerů (pokud budou použity) * Všechny hardwarové komponenty (servery, počítače) a environmentální software používaný v systému. Popis obecné konfigurace hardwaru a vysvětlení, jak se funkce definované ve funkční specifikaci mapují na hardware. * Popis všech částí komponent a uveďte podrobnější informace o hardwarovém a softwarovém prostředí: * primární konfigurace hardwaru * seznam dalších hardwarových konfigurací (např. záložní systémy) * vztah mezi hardwarem a externími rozhraními * seznam veškerého SW potřebného k implementaci a přiřazené k HW * Detailní přehled všech licencí |
| T5 | Struktura systému | * Popis struktury systému, které ukazuje subsystémy a jejich vzájemný vztah. Definice hlavních datových toků mezi subsystémy a hlavními databázovými přístupy * Popis diagramu se shrnutím každého subsystému * Definice součásti systémů a subsystémů a komponent a popis vztahů mezi nimi včetně jejich rozhraní |
| T6 | Architektura databáze | * Popis databáze bez ohledu na to, zda se jedná o SQL nebo non SQL databázi * Definice základních databázové schéma * Popis databázové struktury |
| T7 | Funkční požadavky a jejich řešení | * Popis technického řešení pro každý funkční požadavek konkrétně. Funkční požadavky jsou uvedeny v [Kapitole 5.1 Funkční požadavky](#_Funkční_požadavky) * Ilustrace výstupu funkčních požadavků v podobě řešení a příkladů implementované technologie |
| T8 | Požadavky na architekturu řešení a její implementační řešení rozkreslené v jazyce ArchiMate 3 | * Popis architektury řešení a její rozkreslení v jazyce ArchiMate 3 nebo v jiném adekvátním * Architektura musí obsahovat minimálně všechny komponenty, popis datových toků, služby a popis zajištění vysoké dostupnosti s ohledem na celkovou architekturu |
| T9 | Požadavky na zajištění vysoké dostupnosti a jejích řešení | * Popis řešení vysoké dostupnosti s popisem kritických scénářů a rizik |
| T10 | Škálovatelnost technologického řešení | * Popis, jakým způsobem bude realizována škálovatelnost celého řešení, uvedené na příkladech |
| T11 | Uživatelé | * Popis uživatelů a jejich rolí, definice řešení požadavku na uživatele |
| T12 | Bezpečností požadavky a jejich řešení | * Popis řešení bezpečnostních požadavků |
| T13 | Uživatelské prostředí | * Popis uživatelské prostředí, uveďte řešení všech požadavků a funkcionalit v rámci uživatelského prostředí včetně dashboardu |
| T14 | Postup instalace | * Popis postupu instalace, jednotlivé komponenty, SW a licence |
| T15 | Potřebné součinnosti a jejích rozsah v čase | * Popis veškerých požadavky na součinnost na straně útvarů a rolí na straně SŽ včetně časové posloupnosti požadavků, mimo jiné požadavky na změny konfigurací komunikačních sítí a síťových prvků |
| T16 | Testování a rozsah testů | * Popis testovacích scénářů |
| T17 | Nasazení produkčního prostředí | * Popis způsobu, postupu a posloupnosti v nasazení produkčního prostředí * Popis technických detailů včetně identifikace jednotlivých komponent na úrovní názvů nebo IP adres. |
| T18 | Popis systémů a aplikací které budou nasazeny jako zdroj logů | * Uvedení jmenovitě (dle názvu nebo jiného unikátního identifikátoru) všech instancí systémů nebo technologií, které budou zapojeny do CLM |
| T19 | Popis zpracování logů | * Popis detailně zpracování logů, včetně možnosti korelace, filtrace, obohacování, tvorby událostí, alarmů a všech ostatních funkcionalit životního cyklu logování, požadovaných v rámci funkčních požadavků * Uvedení předpokládané objemy dat a EPS pro plánované zapojení technologií a systémů zpracované na konci analýzy |
| T20 | Popis procesů | * Popis procesů spojených s CLM a s ohledem na prostředí SŽ * Popis minimálně těchto procesů: * Přidání nových typů zdrojů logů nebo integrace nových modulů/funkcí do CLM * Proces s popisem adaptace změn s návazností na stávající change management SŽ v době akceptace projektu * Práce s Logy, nové filtry, vyhledávaní, tvorba události * Tvorba alertu (zohlednit celý životní cyklus od vzniku logu, po jeho zpracování – korelace, enrichment apod. až do vzniku alertu) * Práce s uživateli * Nastavení dashboardu * Odebrání systémů z CLM * Aktualizace systému |
| T21 | Aktualizace systémů | * Popis provádění aktualizací jednotlivých komponent systémů |
| T22 | Předpokládaná rizika a jejích dopady | * Popis technologických/technických rizik spojených s implementaci systému, provozem a jejích dopady |
| T23 | Konfigurační nastavení | * Popis konfiguračního nastavení u těch nastavení, u kterých to bude zřejmé na konci analýzy |
| T24 | Postup obnovy v podobě instalačních kroků a jejích konfigurace | * Popis obnovy v případě selhání systému nebo ztráty dat, současně uveďte způsob nahrání konfigurací |
| T25 | Konkrétní projekt plán s vazbou na Technický návrh implementace | * Popis konkrétního a kompletního projektového plánu s ohledem a vazbou na implementační projekt a potřebné součinnosti |
| T26 | Plnění požadavků dle kybernetického zákona a popis řešení | * Přesná, konkrétní a závazná definice, jakým způsobem budou řešeny všechny požadavky v rámci požadavků dle Zákona č.181/2014 a Vyhlášky č. 82/2018 o kybernetické bezpečnosti * Popis způsob řešení každého požadavku |

## Dodávka SW, HW a licencí

Součástí návrhu dodávky (SW, HW i licencí) a její ceny je zajištění technické podpory a plné funkčnosti po dobu pěti let a to zejména v oblastech:

* Explicitní potvrzení garance výrobce všech komponent CLM o zachování životnosti a plné technické podpory dané komponenty
* Zajištění technické podpory budoucím dodavatelem, specifika jsou uvedena v kapitole [6.13](#_Nadstandardní_služby)

### Dodávka HW

Uchazeč dále navrhne parametry a věcný seznam HW potřebného pro běh všech navržených SW komponent řešení, a to formou přehledové tabulky parametrů s uvedením, zda se musí jednat o dedikovaný HW či virtuální nasazení. Veškerý HW musí být součástí dodávky. Prostor pro montáž HW a stojany budou zajištěny SŽ v rámci vlastních datacenter.

Věcný seznam HW bude přílohou a nedílnou součástí nabídky (konkrétně dokumentu s názvem „Šablona nabídky“). Věcný seznam HW bude obsahovat jednotlivé položky HW, přičemž ke každé položce bude alespoň uvedeno následující:

* jednoznačná specifikace výrobku – uvedením názvu výrobce, názvu (obchodního pojmenování) výrobku a typového čísla výrobku;
* počet kusů dané položky HW, který bude pro kompletní řešení dodán;
* cena jednoho kusu položky a cenu za všechny kusy dané položky, a to vždy bez DPH i s DPH (uvedené ceny budou mít pouze informativní charakter pro představu SŽ o způsobu stanovení nabídkové ceny za dodávku HW).

Součástí dodávky HW bude Software vztahující se k Hardware ve smyslu závazného návrhu Smlouvy a jejích příloh.

### Dodávka SW a licencí

Uchazeč ve své nabídce stanoví a položkově uvede veškeré potřebné SW a licence SW, které budou nutné pro zavedení a správu CLM a zároveň budou součástí dodávky. Dodané licence musí zaručit všechny funkcionality nabízeného CLM.

Seznam potřebného SW a licencí SW bude přílohou a nedílnou součástí nabídky (konkrétně dokumentu s názvem „Šablona nabídky“). Seznam potřebného SW a licencí SW bude obsahovat jednotlivé položky SW a licencí, přičemž ke každé položce bude alespoň uvedeno následující:

* jednoznačná specifikace položky;
* typ SW podle závazného návrhu Smlouvy a jejích příloh – tedy to, zda se jedná o SW v režimu Standardního Software, nebo Unikátního Software;
* rozpad celkové ceny za danou položku (případně pouze celková cena za danou položku SW, pokud se celková cena neskládá z dílčích cen), a to vždy bez DPH i s DPH u každé dílčí ceny i celkové ceny (uvedené ceny budou mít pouze informativní charakter pro představu SŽ o způsobu stanovení nabídkové ceny za dodávku SW a licencí).

## Dodávka Produkčního a testovacího prostředí

SŽ požaduje vybudovaní dvou prostředí – produkčního a vývojového/testovacího. Produkční prostředí bude postupně rozvíjeno v souladu s harmonogramem projektu.

Požadavky na testovací prostředí jsou uvedeny v kapitole [5.1 Funkční požadavky](#_Funkční_požadavky).

## Instalace

Instalace řešení bude provedena do infrastruktury SŽ, která je založena na virtuální platformě, resp. na fyzický server, pokud takový bude Uchazečem v řešení navrhnut. Veškerý HW musí být součástí dodávky.

SW komponenty dodané v rámci řešení budou instalovány v poslední verzi dostupné v době akceptace projektu. Uchazeč dále zajistí nasazení a aktivaci všech licencí, resp. licenčních klíčů. Architektura instalovaného CLM řešení, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace. Instalace je provedena nejprve pro testovací, poté pro produkční prostředí.

## Konfigurace

Uchazeč provede veškerou potřebnou konfiguraci CLM řešení a všech jeho komponent dle požadavků této Technické specifikace včetně součinnosti při konfiguraci sítě. SŽ je odpovědné za zajištění konektivity komunikačních sítí, tj. za provedení změn v konfiguraci síťových prvků.

Uchazeč provede návrh vybraných procesů souvisejících s CLM.

Připojení definovaných zdrojů logů dle navržené etapizace projektu do dodaného CLM řešení.

## Testování

V rámci fáze [Definice Technického návrhu implementace](#_Toc94447636) budou budoucím Dodavatelem navrhnuty testovací scénáře, které budou pokrývat následující oblasti a parametry řešení.

Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad SŽ. Po odstranění významných vad (úroveň středně závažné a více) budou akceptační testy opakovány a ověří tak kvalitu předávaného CLM řešení. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podmínkou akceptace dodávky je provedení všech navržených testů s výsledkem akceptovaným SŽ.

### Funkční testy

Funkční testy ověří, že implementované CLM řešení poskytuje bezchybně všechny požadované funkcionality uvedené v tomto dokumentu a jeho přílohách, včetně řádné integrace s koncovými systémy SŽ. Funkční testy ověří plnou dostupnost koncových systémů dle požadavku na implementaci v rámci jednotlivých etap projektu.

### Zátěžové testy

Zátěžové testy musí být realizovány v takovém rozsahu, aby prostřednictvím stress skriptů ověřily zátěžově celé komplexní řešení v minimálním objemu dvojnásobku standardního provozu.

### Bezpečnostní testy

Úlohou bezpečnostních testů je ověřit, že jsou všechny komponenty zabezpečeny dle požadavků definovaných v tomto dokumentu a přílohách, např. že je zabezpečený přístup k CLM, přístup k logům a nastavení mají pouze autorizované osoby a jejich přístup je logován, zálohy konfigurace a dat jsou řádně šifrovány, uživatelé mají přístup pouze do přidělených bezpečnostních segmentů apod.

Bezpečnostní testy budou realizovány SŽ, nikoliv Budoucím Dodavatelem.

### Sken zranitelností

Provedení skenu zranitelností všech komponent, kde výsledky nesmí obsahovat žádnou zranitelnost, která je hodnocená jako středně závažná nebo horší. Zranitelnosti hodnocené nízkou závažností a nižší mohou být akceptovány SŽ. Pokud nebudou akceptovány, musí budoucí dodavatel zajistit jejich odstranění.

Výsledky všech skenů budou prezentovány pro každou jednotlivou komponentu a musí být akceptovány SŽ.

### Testy zajištění kontinuity

Úlohou testů je ověřit dostupnost CLM řešení v případě výpadku jednotlivých komponent a ověřit jeho funkčnost.

Testování bude provedeno Budoucím Dodavatelem za součinnosti SŽ. Budoucí Dodavatel k realizaci testů zajistí:

* Nástroje a komponenty potřebné pro testování
* Přípravu návrhu testování a hodnotících kritérií
* Přípravu testovacích scénářů
* Přípravu prostředí a testovacích dat (v součinnosti se SŽ)
* Testovací protokoly s výstupy testů
* Seznam defektů a způsob a harmonogram jejich odstranění

## Pilotní provoz

Pilotní provoz bude proveden v produkčním prostředí s cílem otestovat funkčnost CLM v omezeném objemu zdrojových dat, avšak při plné funkcionalitě.

* Budoucí Dodavatel sám navrhne rozsah aktiv pro pilotní provoz. Tento rozsah musí být akceptován SŽ před zahájením pilotního provozu.
* Budoucí Dodavatel navrhne kritéria ukončení pilotního provozu s minimálními požadavky:
  + Pilotní provoz bude realizován minimálně po dobu jednoho měsíce.
  + V rámci pilotního provozu bude začleněno minimálně 10 zdrojů logů z každé skupiny logů.
  + V rámci pilotního provozu bude realizován skutečný provoz CLM, tj. vyhodnocování logů, nikoliv nastavování nebo konfigurace systému samotného.
  + Kritéria ukončení pilotního provozu musí schválit SŽ.
  + Po ukončení Pilotního provozu budou prezentována závěrečná zpráva zástupcům SŽ. Tato zpráva bude obsahovat shrnutí pozorovaných nedostatků, chyb atp., které je nutné odstranit před nasazením CLM do produkčního prostředí v plné funkcionalitě.
* Požadavky na Servisní podporu v režimu SLA musí odpovídat produkčnímu provozu i v pilotním provozu.
* Během pilotního provozu musí být provedena demonstrace přepnutí systémů v rámci HA.
* CLM nemůže být plně spuštěn v produkčním prostředí, dokud nebude SŽ akceptována realizace nápravných opatření vycházejících z pozorování během pilotního provozu.

## Dokumentace

Dokumentace CLM musí obsahovat originální dokumentaci dodanou výrobci všech součástí CLM řešení i dokumentaci popisující nasazení CLM řešení v prostředí SŽ.

Originální dokumentace výrobce všech součástí CLM řešení musí být předána v elektronické podobě (formát PDF nebo MS Word) a musí být provedena v českém nebo anglickém jazyce.

Dokumentace popisující integraci CLM řešení v prostředí SŽ musí být předána v elektronické editovatelné podobě ve formátu MS Word a musí být provedena v českém jazyce.

Dokumentace musí pokrývat minimálně následující oblasti:

* Instalační dokumentace:
  + Popis architektury
  + Komunikační matice komponent
  + Instalované verze
  + Licence
  + Instalační postup pro případ havárie
* Implementační dokumentace:
  + Popis nastavení komponent CLM řešení
  + Popis způsobu integrace (jednotlivých typů koncových systémů)
  + Popis konfigurace zálohování CLM řešení
  + Uživatelská příručka
  + Popis uživatelského rozhraní CLM řešení z pohledu uživatele
  + Popis uživatelských postupů při práci s CLM řešením
* Administrátorská příručka:
  + Popis uživatelského rozhraní CLM řešení z pohledu administrátora
  + Popis základních úkonů nutných pro údržbu CLM řešení a standardní profylaktické testy
  + Popis způsobu aktualizace
  + Popis způsobu modifikace nastavení
  + Popis dodání nebo odebrání nových komponent
  + Popis přidání nových zdrojů logů
* Zajištění kontinuity provozu:
  + Popis postupu obnovy ze zálohy
  + Doporučení pro dlouhodobé ukládání (nahrané uživatelské relace a související data)
  + Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu
* Dokumentace skutečného stavu
* Dokumentace změn a výjimek schválených v průběhu dodávky.

## Školení

Uchazeč musí zajistit proškolení odpovědných osob SŽ na úrovni administrace řešení v rozsahu umožňujícím provádět:

* Běžný rutinní provoz a údržbu dodávaného CLM řešení včetně provedení příslušných konfiguračních změn
* Řešení obvyklých problémů
* Správu uživatelských oprávnění
* Integraci koncového systému
* Analýzu zaznamenaných uživatelských relací
* Monitoring stavu zařízení
* Zálohování a obnovu konfigurace a dat
* Tvorbu pohledů a reportů

Školení musí být v rozsahu min 32 vyučovacích hodin na každou roli. Musí být vykonáno prezenčně, včetně praktických cvičeních na systému a musí být zakončeno testem.

## Předání do provozu

Uchazeč musí zajistit předání plného CLM řešení do produkčního užívání (již fáze [Pilotního provozu](#_Pilotní_provoz) bude provozována v produkčním prostředí).

Před předáním CLM do produkčního užívání musí být splněna všechna akceptační kritéria vycházející z předcházejících kapitol ([6.1](#_Definice_konceptu) až [6.10](#_Školení)), která musí být písemně akceptována SŽ.

## Zajištění technické podpory provozu

Uchazeč musí zaručit, že CLM řešení bude funkční a použitelné v prostředí SŽ a bude odpovídat požadavkům uvedeným v Technickém návrhu implementace a vlastnostem deklarovaným v dokumentaci výrobce dodané uchazečem.

Předmětem technické podpory je poskytování expertních služeb, které budou využívány zejména pro podporu činností SŽ v případě problémů s dodaným řešením a jako doplněk k zajištění odborné pomoci v případech vyžadujících expertní znalost.

Měření SLA bude realizováno na straně SŽ, prostřednictvím jeho servisdeskového systému.

Technická podpora provozu musí být v souladu se závazným návrhem smlouvy a jejími přílohami, tj. zejména se standardizovaným dokumentem SŽ – Zvláštní obchodní podmínky pro Zakázky v oblasti ICT.

## Nadstandardní služby

Maximální souhrn nadstandardních služeb bude činit ročně 120 MD dle konkrétních potřeb pro rozložení čerpání SŽ.

SŽ požaduje uvést cenu za následující položky ve formě ceny za 1MD a celkové ceny za položku podle předpokládaného objemu čerpání:

|  |  |
| --- | --- |
| Položka | Předpokládané čerpání v MD za rok |
| Konzultace nad rámec paušálu, tj. nad rámec základních služeb poskytnutých v projektu | 25 |
| Zásah v lokalitě SŽ na vyžádání, mimo servisní smlouvu | 25 |
| Školení nad rámec základních školení | 10 |
| Změnová řízení a dovývoj | 60 |

Celková cena za výše uvedené položky musí být součástí cenové nabídky Budoucího Dodavatele.