

**Národní památkový ústav**, státní příspěvková organizace  
IČO: 75032333, DIČ: CZ75032333,  
se sídlem: Valdštejnské nám. 162/3, PSČ 118 01 Praha 1 – Malá Strana,  
zastoupen: Ing. arch. Naděždou Goryczkovou, generální ředitelkou  
bankovní spojení: Česká národní banka, č. ú.: 60039011/0710  
(dále jen „**kupující**“)

a

**BIT SERVIS spol. s r.o.**

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, vložka C, oddíl 11262  
se sídlem: Libušská 144/252, 142 00 Praha  
IČO: 45793972, DIČ: CZ45793972  
zastoupená: Ondřejem Koutským, jednatelem  
bankovní spojení: xxxxxxxxxxxxxxxx, č. ú.: xxxxxxxxxxxxxxxx  
(dále jen „**prodávající**“)

jako smluvní strany uzavřely níže uvedeného dne, měsíce a roku ve smyslu ust. § 2085 a násl. zák. č. 89/2012 Sb., občanský zákoník, v platném znění následující

**kupní smlouvu:**

**Článek I.**

**Úvodní ustanovení**

1. Smluvní strany konstatují, že tuto smlouvu uzavírá kupující s prodávajícím na základě veřejné zakázky malého rozsahu s názvem „**Dodávka a implementace centrálního úložiště logů**“, ID zakázky přidělené systémem Národního elektronického nástroje: N006/18/V00012807. Smluvní strany se dohodly, že závaznou část jejich smluvních ujednání tvoří rovněž nabídka prodávajícího a zadávací dokumentace na veřejnou zakázku.

**Článek II.**

**Předmět smlouvy**

1. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu v souladu se zadávacími podmínkami a zadávací dokumentací veřejné zakázky uvedené v čl. I této smlouvy a s nabídkou prodávajícího jako vítězného uchazeče o tuto veřejnou zakázku **centrální úložiště logů podle specifikace uvedené v příloze č. 1 této smlouvy, včetně jeho implementace** (dále jen „**zboží**“), a převést na kupujícího vlastnické právo ke zboží, a závazek kupujícího převzít zboží do vlastnictví České republiky s příslušností hospodařit pro kupujícího a zaplatit prodávajícímu sjednanou kupní cenu podle článku VII. této smlouvy.
2. Předmět této smlouvy je dále závazek prodávajícího poskytnout kupujícímu servisní a technickou podporu dle podmínek stanovených touto smlouvou a přílohou č. 1 této smlouvy.

**Článek III.**

**Místo a doba dodání, přechod vlastnického práva**

1. Prodávající se zavazuje dodat kupujícímu zboží specifikované blíže v příloze č. 1 smlouvy, a to do 3 měsíců ode dne účinnosti této smlouvy.
2. Místem plnění je: sídlo kupujícího na adrese: Valdštejnské nám. 162/3, PSČ 118 01 Praha 1 – Malá Strana.
3. Zboží je dodáno v okamžiku převzetí zboží kupujícím v místě plnění.
4. Prodávající výslovně prohlašuje, že zboží bude dodáno v ujednaném množství, jakosti a provedení, včetně příslušných dokladů nutných k užívání věci, bude prosté faktických i právních vad a způsobilé k užívání. Zboží bude dodáno kupujícímu jako nové, nepoužité a bez vad.
5. O převzetí zboží bude smluvními stranami sepsán předávací protokol.

6. Prodávající je povinen informovat pověřeného zástupce kupujícího uvedeného v čl. X smlouvy telefonicky nebo emailem o dodání zboží na místo plnění a dohodnout s ním konkrétní den a hodinu dodání nejméně 3 pracovní dny předem.
7. Vlastnické právo k předmětu koupě kupující nabývá jeho převzetím. Nebezpečí škody na věci přechází na kupujícího rovněž jeho převzetím.

#### **Článek IV.**

##### **Implementační práce**

1. Součástí dodávky budou následující činnosti instalace a konfigurace dodaného řešení:
  - Instalace do racku v datovém centru zadavatele (Praha)
  - Základní konfigurace LAN, ověřování uživatelů, NTP, SMTP, instalace certifikátů, konfigurace prostředí domény Active Directory
  - Konfigurace serverů Windows pro logování do prostředí log management serveru včetně textových logů (DHCP, IIS, NAP ...) (cca 50 ks)
  - Konfigurace serverů Linux pro logování do prostředí log management serveru (cca 30 ks)
  - Konfigurace databázových serverů (MS SQL, Oracle, PostgreSQL, Firebird) pro logování do prostředí log management serveru (cca 7 ks)
  - Konfigurace doménových politik pro auditování serverů Windows a fileserverů
  - Konfigurace přepínačů Cisco pro logování do prostředí log management serveru (cca 5 kusů)
  - Konfigurace přepínačů Cisco SG pro logování do prostředí log management serveru (cca 30 kusů)
  - Konfigurace firewallů Cisco ASA pro logování do prostředí log management serveru (3 kusy)
  - Konfigurace firewallů CheckPoint pro logování do prostředí log management serveru (2 kusy)
  - Konfigurace management rozhraní serverů IBM/Lenovo pro logování do prostředí log management serveru (3 kusy)
  - Konfigurace management rozhraní IBM/Lenovo Flex šasi včetně serverů a síťových přepínačů pro logování do prostředí log management serveru (cca 3 ks)
  - Konfigurace diskových polí IBM/Lenovo storwize pro logování do prostředí log management serveru (4 kusy)
  - Konfigurace EMC datadomain pro logování do prostředí log management serveru (2 ks)
  - Vytvoření parserů pro disková pole IBM/Lenovo storwize v prostředí log management serveru
  - Vytvoření parserů pro servery IBM/Lenovo v prostředí log management serveru
  - Vytvoření parserů pro IBM/Lenovo Flex šasi v prostředí log management serveru
  - Vytvoření parserů pro EMC datadomain v prostředí log management serveru
  - Vytvoření parserů pro Veeam backup v prostředí log management serveru
  - Vytvoření parserů pro aplikační servery v prostředí log management serveru (cca 40 aplikací)
  - Vytvoření parseru pro telefonní ústřednu Mitel MiVoice MX-ONE v prostředí log management serveru
  - Vytvoření dashboardu pro sledování diskových polí IBM/Lenovo storwize v prostředí log management serveru
  - Vytvoření dashboardu pro sledování serverů a Flex šasi IBM/Lenovo v prostředí log management serveru
  - Vytvoření dashboardu pro sledování EMC datadomain v prostředí log management serveru
  - Vytvoření dashboardů pro sledování Veeam backup v prostředí log management serveru
  - Vytvoření dashboardů pro sledování telefonní ústředny Mitel MiVoice MX-ONE v prostředí log management serveru
  - Podpora aplikačních partnerů při konfiguraci logování aplikačních serverů do prostředí log management serveru (cca 40 aplikací)
  - Podpora konfigurace telefonní ústředny Mitel MiVoice MX-ONE pro logování do prostředí log management serveru
  - Vytvoření alertů pro oznamování vzniku kritických událostí
  - Optimalizace zpracovávání logů v prostředí log management serveru
  - Konfigurace přístupu administrátorů a externích dodavatelů k zaznamenaným událostem

- Školení administrátorů pro práci v prostředí log management serveru a statistické zpracování zaznamenaných událostí
  - Školení vybraných administrátorů pro práci s programovacím nástrojem log management serveru
2. Místem plnění implementace je: sídlo kupujícího na adrese: Valdštejnské nám. 162/3, PSČ 118 01 Praha 1 – Malá Strana, a datové centrum kupujícího v DC TOWER v Praze. Činnosti, které to svým charakterem umožňují, lze realizovat prostřednictvím vzdáleného přístupu.
  3. O řádném provedení implementace bude smluvními stranami sepsán písemný protokol.
  4. Implementace ve výše uvedeném rozsahu bude provedena do 3 měsíců od data účinnosti smlouvy.

#### **Článek V.**

##### **Odpovědnost za vady, záruka a záruční podmínky, servis**

1. Prodávající poskytuje záruku na dodaný hardware (zboží) v délce 60 měsíců a servisní podporu s opravou v místě instalace a s garantovanou odezvou následující pracovní den od nahlášení závady.
2. Prodávající dále poskytuje záruku na dodaný software v délce 60 měsíců a servisní podporu zahrnující: aktualizaci software (min. jednou ročně), opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.
3. Záruční doba začíná běžet ode dne převzetí zboží kupujícím a podpisem předávacího protokolu, přičemž záruční doba neběží po dobu, po kterou kupující nemůže zboží užívat pro jeho vady, za které odpovídá prodávající.
4. Hlášení závad a jiných incidentů: Kupující nahlásí prodávajícímu vadu či jiný incident - telefonicky: +420 xxxxxxxxxxxx /na email: xxxxxxxxxxxx /na helpdesk prodávajícího dostupný online prostřednictvím Internetu na adrese <https://bitservis.freshdesk.com>.
5. Prodávající je povinen odstranit bez prodloužení a bezplatně zjištěné vady (nedohodnou-li se strany jinak, musí vady odstranit do 15 pracovních dnů).

#### **Článek VI.**

##### **Postimplementační podpora**

1. Předmětem této smlouvy je dále závazek prodávajícího poskytnout postimplementační podporu zahrnující především následující činnosti:
  - úpravy konfigurace dodaného řešení,
  - podpora při řešení servisních požadavků a oprav a při instalaci softwarových aktualizací dodaného řešení,
  - úpravy stávajících a vytváření nových parserů a dashboardů pro další zařízení a aplikace zadavatele,
  - podpora aplikačních partnerů při konfiguraci logování do prostředí log management serveru,
  - optimalizace funkcionality celého řešení,
  - implementace řešení pro sběr událostí z poboček,
  - školení a podpora administrátorů zadavatele.
2. Postimplementační podpora bude poskytována po celé období trvání záruky podle této smlouvy.
3. Konkrétní plnění jednotlivých činností dle tohoto článku budou vždy předmětem samostatné objednávky vystavené kupujícím po předchozím projednání a odsouhlasení rozsahu požadovaných činností a hodin ze strany prodávajícího a ujednání termínu plnění.

#### **Článek VII.**

##### **Cena a platební podmínky**

1. Kupní cena za dodání zboží (specifikovaného v čl. II a příloze č. 1, včetně implementace dle čl. IV a záruční servisní podpory dle čl. V. této smlouvy) byla dle dohody prodávajícího a kupujícího stanovena:

Cena bez DPH:	1.032.450,-Kč
DPH ve výši 21%	216.815,-Kč
Celková cena včetně DPH	1.249.265,- Kč.

2. Pokud bude prodávajícím prováděna činnost postimplementační podpory dle článku VI. této smlouvy, je její cena odvozena na základě domluvených hodinových sazeb:

Cena:	1.350,- Kč bez DPH/hodinu
Cena dopravy:	0,- Kč bez DPH/km (doprava nebude účtována, je součástí hodinové sazby)

Tyto ceny zahrnují veškeré související náklady a výlohy (cestovné apod.) a jsou neměnné po celou dobu trvání smlouvy.

- Sjednaná kupní cena je konečná a nepřekročitelná a zahrnuje veškeré náklady na splnění dodávky předmětu koupě dle této smlouvy, včetně nákladů na dopravu předmětu koupě na místo převzetí.
- Kupní cena dle odst. 1 bude zaplacená po převzetí zboží kupujícím a provedení implementačních prací, tj. po podpisu předávacího protokolu, na základě faktury vystavené prodávajícím, se splatností do 21 dní od doručení daňového dokladu.
- Úhrada za postimplementační podporu dle čl. VI. této smlouvy bude uhrazena na základě daňového dokladu vystaveného prodávajícím, který bude odpovídat objednavce.
- Daňový doklad musí obsahovat všechny náležitosti řádného účetního a daňového dokladu dle příslušných právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, dále musí splňovat smlouvou stanovené náležitosti, jinak je kupující oprávněn jej vrátit s tím, že prodávající je poté povinen vystavit nový s novým termínem splatnosti. V takovém případě není kupující v prodlení s úhradou.
- Kupující je oprávněn provést zajišťovací úhradu DPH na účet příslušného finančního úřadu, jestliže se prodávající stane ke dni uskutečnění zdanitelného plnění nespolehlivým plátcem dle zákona o dani z přidané hodnoty.
- Prodávající prohlašuje, že ke dni podpisu smlouvy není veden jako nespolehlivý plátcem dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, a zavazuje se, že se jím nestane po celou dobu trvání jakýchkoliv finančních závazků plynoucích z této smlouvy. Prodávající se dále zavazuje uvádět pro účely bezhotovostního převodu pouze účet či účty, které jsou správcem daně zveřejněny způsobem umožňujícím dálkový přístup dle zákona o dani z přidané hodnoty. V případě, že se přesto prodávající stane nespolehlivým plátcem, je povinen tuto skutečnost oznámit NPÚ neprodleně (nejpozději do 3 dnů ode dne, kdy se jím stal) na email uvedený u kupujícího v hlavičce této smlouvy. V případě porušení oznamovací povinnosti je prodávající povinen uhradit kupujícímu jednorázovou smluvní pokutu ve výši částky odpovídající výši DPH připočtené k ceně předmětu koupě.

### Článek VIII.

#### Sankční ujednání

- V případě prodlení prodávajícího s dodáním zboží v termínu podle čl. III a/nebo provedením implementace v termínu podle čl. IV se smluvní strany dohodly na smluvní pokutě ve výši 0,25% z celkové kupní ceny vč. DPH dle čl. VII odst. 1 za každý, byť i započatý, den prodlení.
- V případě nedodržení podmínek záručního servisu podle čl. V se smluvní strany dohodly na smluvní pokutě ve výši 1.000,- Kč za každý, byť i započatý, den prodlení, a to pro každý případ reklamace zvlášť, případně za každý jednotlivý případ porušení povinnosti záručního servisu (v závislosti na povaze plnění).
- Pro případ prodlení prodávajícího s provedením postimplementační podpory za podmínek sjednaných objednávkou dle čl. VI. této smlouvy má objednatel právo účtovat smluvní pokutu ve výši 500,- Kč bez DPH za každý započatý den prodlení.
- V případě prodlení kupujícího se zaplacení dohodnuté ceny na základě řádně vystavené faktury prodávajícího v souladu s čl. VII této smlouvy sjednávají smluvní strany zákonný úrok z prodlení za každý, byť započatý, den prodlení.
- V případě svévolného předčasného ukončení smlouvy kteroukoliv ze smluvních stran si smluvní strany sjednaly smluvní pokutu ve výši 50.000,- Kč.

6. Smluvní pokuty dle této smlouvy jsou splatné do 21 dnů po obdržení vyúčtování smluvní pokuty. Strany si sjednávají, že ve vztahu k náhradě škody vzniklé porušením smluvní povinnosti platí, že právo na její náhradu není zaplacením smluvní pokuty dotčeno. Odstoupením od smlouvy není dotčen nárok na zaplacení smluvní pokuty ani nároky na náhradu škody. Kupující je oprávněn, zejména v případě, kdy prodávající ve stanovené lhůtě neuhradí smluvní pokutu, započíst na své závazky vůči prodávajícímu své finanční nároky na smluvní pokutu, kterou prodávajícímu vyúčtuje.

#### **Článek IX.**

##### **Trvání smlouvy, odstoupení od smlouvy**

1. Tato smlouva se uzavírá na dobu určitou, a to ode její účinnosti na dobu 63 měsíců.
2. Kupující je oprávněn od této smlouvy odstoupit:
  - v případě prodlení prodávajícího s dodáním zboží v termínu podle čl. III a/nebo provedením implementace v termínu podle čl. IV této smlouvy,
  - v případě nedodržení podmínek záručního servisu podle čl. V s tím, že prodávající nesjednává nápravu ani v dodatečně přiměřené lhůtě poskytnuté kupujícím (není-li sjednáno jinak, považuje se přiměřenou lhůtu 15 pracovních dní),
  - v případě prodlení prodávajícího s provedením postimplementační podpory za podmínky sjednaných objednávkou dle čl. IV. této smlouvy,
  - v případě jiného podstatného porušení smlouvy.
3. Proávající je oprávněn od této smlouvy odstoupit písemným odstoupením:
  - v případě prodlení kupujícího se zaplacením dohodnuté ceny na základě řádně vystavené faktury prodávajícího v souladu s čl. VII této smlouvy, trvajícího déle než 30 dní,
  - v případě jiného podstatného porušení smlouvy.
4. Odstoupení od smlouvy je účinné dnem následujícím po doručení odstoupení druhé smluvní straně.

#### **Článek X.**

##### **Pověření pracovníci**

1. Za kupujícího:
  - a. xxxxxxxxxxxx, vedoucí odboru informatiky, tel.: xxxxxxxxxxx, e-mail: xxxxxxxxxxxx
  - b. xxxxxxxxxxxx vedoucí odd. provozní informatiky a správy ICT, tel.: xxxxxxxxxxxx, e-mail: xxxxxxxxxxxx
  - c. xxxxxxxxxxxx, správce ICT, tel.: xxxxxxxxxxxx, e-mail: xxxxxxxxxxxx
2. Za prodávajícího:
  - a. xxxxxxxxxxxx, obchodník, tel.: xxxxxxxxxxxx, e-mail: xxxxxxxxxxxx
  - b. xxxxxxxxxxxx, jednatel, tel.: xxxxxxxxxxxx, e-mail: xxxxxxxxxxxx
  - c. xxxxxxxxxxxx, technik, tel.: xxxxxxxxxxxx, e-mail: xxxxxxxxxxxx
3. V případě, že dojde u některé ze smluvních stran ke změně odpovědné osoby, oznámí změnu této odpovědné osoby písemně druhé smluvní straně. Účinnost změny odpovědné osoby vůči druhé smluvní straně nastává okamžikem doručení tohoto oznámení. Oznámení o změně odpovědné osoby se nepovažuje za změnu této smlouvy.

#### **Článek XI.**

##### **Závěrečná ustanovení**

1. Proávající se vzdává svého práva namítat nepřiměřenou výši smluvní pokuty u soudu ve smyslu § 2051 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
2. Tato smlouva byla sepsána ve dvou vyhotoveních. Každá ze smluvních stran obdržela po jednom totožném vyhotovení.
3. Smluvní strany berou na vědomí, že tato smlouva podléhá povinnosti uveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv); povinnost uveřejnění zajistí kupující.
4. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami a účinnosti dnem uveřejnění v registru smluv.

5. Smluvní strany berou na vědomí, že tato smlouva může být předmětem zveřejnění i dle jiných právních předpisů.
6. Smluvní strany se zavazují spolupůsobit jako osoba povinná v souladu se zákonem č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů.
7. Informace k ochraně osobních údajů jsou ze strany NPÚ uveřejněny na webových stránkách [www.npu.cz](http://www.npu.cz) v sekci „Ochrana osobních údajů“.
8. Smlouvu je možno měnit či doplňovat výhradně písemnými číslovanými dodatky.
9. Smluvní strany prohlašují, že tuto smlouvu uzavřely podle své pravé a svobodné vůle prosté omylů, nikoliv v tísní a že vzájemné plnění dle této smlouvy není v hrubém nepoměru. Smlouva je pro obě smluvní strany určitá a srozumitelná.

V Praze, dne

V Praze, dne

.....  
Ing. arch. Naděžda Goryczková  
generální ředitelka

.....  
Ondřej Koutský  
jednatel

## Příloha číslo 1 Smlouvy

### POPIS A TECHNICKÁ SPECIFIKACE NABÍZENÉHO ŘEŠENÍ

Uchazeč BIT SERVIS spol. s r.o. navrhuje a nabízí řešení LOGmanager od českého výrobce Sirwisa a.s., a to konkrétně produkt s označením LOGM-48TB-DELL-5Y (velký LOGmanager). Tento model bude dodán včetně 5leté HW záruky a 5leté SW podpory. Celé řešení naistalují naši techničtí pracovníci a následně předají k užívání zadavateli. Součástí předání bude také zaškolení dle požadavků zadavatele.

**Uchazeč BIT SERVIS potvrzuje, že nabízené řešení splňuje bez výjimky v plné šíři všechny požadavky uvedené v příloze a pod č. 1-85.** Jako potvrzení vkládáme níže tabulku Zadavatele obohacenou o sloupec s vyjádřením, zda nabízené řešení LOGmanager splňuje či nesplňuje požadovaný parametr.

**Uchazeč BIT SERVIS potvrzuje, že nabízené řešení a cenová nabídka zahrnuje Požadavky na záruky v následujícím rozsahu:**

- 5-letá servisní podpora na dodaný hardware s opravou v místě instalace a s garantovanou odezvou následující pracovní den od nahlášení závady
- 5-letá SW podpora výrobce, která obsahuje aktualizaci software, opravy chyb a telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

**Uchazeč BIT SERVIS potvrzuje, že cenová nabídka zahrnuje Požadavky na implementační práce v následujícím rozsahu:**

- Instalace do racku v datovém centru zadavatele (Praha)
- Základní konfigurace LAN, ověřování uživatelů, NTP, SMTP, instalace certifikátů, konfigurace prostředí domény Active Directory
- Konfigurace serverů Windows pro logování do prostředí log management serveru včetně textových logů (DHCP, IIS, NAP ...) (cca 50 ks)
- Konfigurace serverů Linux pro logování do prostředí log management serveru (cca 30 ks)
- Konfigurace databázových serverů (MS SQL, Oracle, PostgreSQL, Firebird) pro logování do prostředí log management serveru (cca 7 ks)
- Konfigurace doménových politik pro auditování serverů Windows a fileserverů
- Konfigurace přepínačů Cisco pro logování do prostředí log management serveru (cca 5 kusů)
- Konfigurace přepínačů Cisco SG pro logování do prostředí log management serveru (cca 30 kusů)
- Konfigurace firewallů Cisco ASA pro logování do prostředí log management serveru (3 kusy)
- Konfigurace firewallů CheckPoint pro logování do prostředí log management serveru (2 kusy)
- Konfigurace management rozhraní serverů IBM/Lenovo pro logování do prostředí log management serveru (3 kusy)
- Konfigurace management rozhraní IBM/Lenovo Flex šasi včetně serverů a síťových přepínačů pro logování do prostředí log management serveru (cca 3 ks)
- Konfigurace diskových polí IBM/Lenovo storwize pro logování do prostředí log management serveru (4 kusy)
- Konfigurace EMC datadomain pro logování do prostředí log management serveru (2 ks)
- Vytvoření parserů pro disková pole IBM/Lenovo storwize v prostředí log management serveru
- Vytvoření parserů pro servery IBM/Lenovo v prostředí log management serveru
- Vytvoření parserů pro IBM/Lenovo Flex šasi v prostředí log management serveru
- Vytvoření parserů pro EMC datadomain v prostředí log management serveru
- Vytvoření parserů pro Veeam backup v prostředí log management serveru
- Vytvoření parserů pro aplikační servery v prostředí log management serveru (cca 40 aplikací)
- Vytvoření parseru pro telefonní ústřednu Mitel MiVoice MX-ONE v prostředí log management serveru
- Vytvoření dashboardu pro sledování diskových polí IBM/Lenovo storwize v prostředí log management serveru
- Vytvoření dashboardu pro sledování serverů a Flex šasi IBM/Lenovo v prostředí log management serveru
- Vytvoření dashboardu pro sledování EMC datadomain v prostředí log management serveru

- Vytvoření dashboardů pro sledování Veeam backup v prostředí log management serveru
- Vytvoření dashboardů pro sledování telefonní ústředny Mitel MiVoice MX-ONE v prostředí log management serveru
- Podpora aplikačních partnerů při konfiguraci logování aplikačních serverů do prostředí log management serveru (cca 40 aplikací)
- Podpora konfigurace telefonní ústředny Mitel MiVoice MX-ONE pro logování do prostředí log management serveru
- Vytvoření alertů pro oznamování vzniku kritických událostí
- Optimalizace zpracovávání logů v prostředí log management serveru
- Konfigurace přístupu administrátorů a externích dodavatelů k zaznamenaným událostem
- Školení administrátorů pro práci v prostředí log management serveru a statistické zpracování zaznamenaných událostí
- Školení vybraných administrátorů pro práci s programovacím nástrojem log management serveru
- 

**Uchazeč BIT SERVIS potvrzuje, že cenová nabídka zahrnuje Požadavky na post implementační podporu v následujícím rozsahu:**

Nedílnou součástí dodávky je dále postimplementační podpora v období 5-leté HW a SW záruky dodaného řešení, která bude zahrnovat především následující činnosti:

- úpravy konfigurace dodaného řešení
- podpora při řešení servisních požadavků a oprav a při instalaci softwarových aktualizací dodaného řešení
- úpravy stávajících a vytváření nových parserů a dashboardů pro další zařízení a aplikace zadavatele
- podpora aplikačních partnerů při konfiguraci logování do prostředí log management serveru
- optimalizace funkcionality celého řešení
- implementace řešení pro sběr událostí z poboček
- školení a podpora administrátorů zadavatele

## Podrobný popis řešení LOGmanager

LOGmanager je HW řešení pro centralizovanou správu logů a jiných strojových dat z libovolných zdrojů. Je založen na výkonné databázi s obrovskou kapacitou, rychlým vyhledáváním ve "velkých datech" a okamžitou vizualizací vyžádaných dat. Jeho podstatou je sběr, dlouhodobé nezpochybnitelné ukládání a analýza strojových dat organizace. Umožňuje prohledávat agregovaná velká data v reálném čase, vytvářet statistické analýzy, reporty a upozornění na události korelované z dat více zdrojů. Při správné implementaci pomůže organizaci k zajištění shody s ČSN/ISO 27001:2013 o pořizování auditních záznamů, plnění požadavků GDPR. Při vývoji LOGmanageru je kladen velký důraz na jeho reálný přínos pro IT. Toto řešení je velkou pomocí pro provoz IT obecně, protože na jednom místě shromáždí provozní data ze všech důležitých systémů. Operátor IT tak dostane možnost zjistit během několika sekund informace o provozních stavech a případných závadách, které by jinak musel hodiny komplikovaně vyhledávat v distribuovaných zdrojích. K tomu je i automaticky informován o sledovaných událostech a může tak předcházet kritickým IT nebo bezpečnostním incidentům.

LOGmanager nativně podporuje více než 120 zdrojů ze všech oblastí IT, od bezpečnostních řešení, přes síťové prvky, virtualizace, operační systémy, databáze až po aplikace. Seznam je velmi široký a s každou aktualizací se rozšiřuje. LOGmanager dále podporuje standardizované strukturované formáty logů jako jsou CEF, LEEF a JSON. Pro specifické zdroje umožňuje rychlé a snadné vytvoření zákaznických parserů.

Klíčovými vlastnostmi LOGmanageru jsou:

- Centrální úložiště logů, událostí a strojových dat organizace
- Sjednocení formátu zdrojových logů do lidsky srozumitelné formy
- Zpracování a vizualizace přijímaných dat v reálném čase
- Rychlé prohledávání dat bez nutnosti znalosti SQL jazyka
- SIEM funkce. Alerty na základě podmínek s limity a korelacemi
- Unikátní grafické konfigurační a programovací rozhraní
- Radikální jednoduchost a uživatelská přívětivost
- Snadné vytváření reportů a auditních zpráv za běhu
- Umožní snadnější splnění požadavku na shodu s regulacemi pro:
  - GDPR
  - Zákon o kybernetické bezpečnosti a návazné vyhlášky
  - ČSN/ISO 27001:2013 pro pořizování auditních záznamů
  - PCI DSS 3.2
- Bez licenčních omezení na množství zdrojů, výkon a uložená data

Technické parametry LOGmanager:

LOGmanager Appliance								
CPU	Memory	Disk	RAID	DB Capacity	Data Retency (Average EPS*-days)	MAX Constant EPS*	Peak EPS*	Cluster Support
<b>Velký LOGmanager</b>								
2x10core Intel Xeon 2.2GHz	128B	12*4TB	6	40TB	3000EPS*-275days	5000-6000	10000/10min	Ano, 2 units
EPS* - Average Events Per Second RAW log size 700Byte; Data Retency - counted for Average 24*7 Constant EPS rate								

**Technická specifikace – tabulka splňuje (ANO/NE)**

Tato technická specifikace je tabulka ze zadávací dokumentace Zadavatele „Příloha\_a\_Logmanagement\_Bližší specifikace plnění“ doplněná o sloupec s vyjádřením, zda řešení LOGmanager uvedený parametr splňuje či nikoliv.

Číslo	Popis	Splňuje (ANO/NE)
<b>Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat</b>		
1	Systém pracuje jako appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti.	ANO
2	Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware (nejméně v rozsahu seznamu podporovaných zařízení a systémů v Příloze č. 1 této Bližší specifikace předmětu plnění - Seznam podporovaných systémů).	ANO
3	Systém umožňuje pro zařízení neuvedená v seznamu podporovaných zařízení dopsání parseru uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem nabízeného systému - uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce.	ANO
4	Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožňovat přijímat logy i na uživatelsky definovaných UDP a TCP portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.	ANO
5	Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí.	ANO
6	Všechny normalizované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	ANO
7	Systém umožňuje sběr událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159.	ANO
8	Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	ANO
9	Systém provádí konsolidaci logů na centrálním místě.	ANO
10	Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.	ANO
11	Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj. volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle nastavené volby automaticky.	ANO
12	Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období.	ANO
13	Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace.	ANO
14	Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám.	ANO
15	V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.	ANO
16	Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.	ANO
17	Systém musí splňovat požadavky normy ISO 27001:2014 na pořizování auditních	ANO

	záznamů.	
18	Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění dat.	ANO
19	Systém má možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí použití.	ANO
20	Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů na data. Reporty musí být možné exportovat mimo systém do běžnými nástroji zobrazitelných formátů. Pro vytváření nových pohledů na data není přípustné vyžadovat povinně SQL jazyk.	ANO
21	Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.	ANO
22	Konfigurační a Systémové rozhraní a On-line dokumentace je poskytována a je obsahově identická nejméně v anglickém a v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce.	ANO
23	Systém nabízí kapacitní i výkonovou škálovatelnost.	ANO
24	Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.	ANO
25	Systém umožňuje, aby z diskového pole bylo možné vytáhnout libovolné dva disky, bez ztráty dat a bez vlivu na funkčnost řešení. Redundance disků neovlivňuje požadovanou kapacitu úložiště.	ANO
26	Systém umožňuje on-line Monitoring stavu - alertování při překročení prahových hodnot nebo při chybě systému. Upozornění zasílá pomocí SMTP nebo Syslog.	ANO
27	Systém obsahuje REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG, případně další) a umožňuje autorizovaný přístup ke strukturované databázi logů.	ANO
28	Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou výjimkou je monitorování systémů Windows, které přes WMI protokol neumožňují monitorovat textové logy.	ANO
29	Systém obsahuje jednotnou centrální webovou konzoli pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému.	ANO
30	Systém umožňuje snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.	ANO
31	Systém podporuje ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému podporuje ověření z lokální databáze.	ANO
<b>Minimální HW parametry požadovaného systému</b>		
32	Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	ANO
33	HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.	ANO
34	Systém obsahuje min. 2 procesory (min. 10 jader každý), s podporou HyperThreadingu.	ANO
35	Systém obsahuje operační paměť RAM min. 128 GB DDR-4.	ANO
36	Systém disponuje úložištěm o velikosti minimálně 40TB pro integrovanou databázi podporovanou HW akceleračním SAS RAID řadičem s read-write cache (min. 2GB). Řadič diskového pole obsahuje zálohovací baterii nebo je vybaven flash pamětí.	ANO
37	Systém obsahuje minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček (výkonové důvody).	ANO
38	Systém obsahuje minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.	ANO

39	Větráky v systému musí být vyměnitelné za provozu a redundantní.	ANO
40	Systém obsahuje 2x napájecí zdroje s redundancí napájení 1+1.	ANO
41	Systém obsahuje virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače).	ANO
42	Systém obsahuje vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdobá HP iLO, Dell iDRAC apod).	ANO
<b>Výkonnostní a SW parametry systému</b>		
43	Systém je nabízen a bude dodán ve formě appliance - v rámci jednoho HW stroje obsahuje všechny části systému, jež je možné nastavit v centrální správčovské konzoli - viz bod 29.	ANO
44	Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správčovskou konzoli (viz bod 29).	ANO
45	Systém umožňuje průměrný trvalý příjem min. 5 tis. událostí/s s možností navýšení formou upgrade na minimálně 10 tis. událostí/s prostřednictvím licence nebo rozšíření hardware.	ANO
46	Systém umožňuje špičkový příjem 10 tis. událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. Po volitelném licenčním nebo hardware zvýšení výkonu pak 20 tis. událostí/s po dobu nejméně 10 minut.	ANO
47	Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den, nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat.	ANO
48	Systém nabízí uživatelskou konfiguraci vlastních parserů pomocí vizuálního programovacího jazyka v centrální správčovské webové konzoli (viz bod 29). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování.	ANO
49	Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.	ANO
50	Systém umožňuje on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat.	ANO
51	V centrální správčovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.	ANO
52	V centrální správčovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).	ANO
53	Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	ANO
54	Systém podporuje zrcadlení a provoz v clusteru – 2 a více zařízení v režimu active / active.	ANO
55	Vícenodový systém se chová jako 1 celek.	ANO
56	V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.	ANO
57	Systém umožňuje rozšiřování kapacity i navýšování výkonu pomocí přidávání dalších zařízení do clusteru.	ANO
58	V případě rozšíření na cluster (přidání dalšího node) musí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody.	ANO

59	Systém podporuje zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.	ANO
<b>Alerty</b>		
60	Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.	ANO
61	Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparované události.	ANO
62	Systém obsahuje výrobcem předpřipravené sety/vzory alertů.	ANO
63	Konfigurace alertů je prováděna pomocí vizuálního programovacího jazyka.	ANO
64	V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha).	ANO
65	Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity.	ANO
66	Jako výstupní pravidlo alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol.	ANO
<b>Sběr událostí z Microsoft prostředí</b>		
67	Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů.	ANO
68	Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.	ANO
69	Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole z bodu 29.	ANO
70	Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.	ANO
71	Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy (z důvodu, že správce logovacího systému není zároveň správce domény).	ANO
72	Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).	ANO
73	Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.	ANO
74	Komunikace Windows agenta a centrálního systému musí být šifrovaná.	ANO
75	Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.	ANO
76	Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.	ANO
77	Počet instalací Windows agenta nesmí být licenčně omezen.	ANO
<b>Podpora pro sběr událostí z poboček</b>		
78	Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.	ANO
79	Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášena data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	ANO

80	Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.	ANO
81	Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.	ANO
82	Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí/s a to i v trvalé zátěži.	ANO
83	Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.	ANO
84	Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.	ANO
85	Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).	ANO

### Seznam podporovaných systémů

Podpora přímého načítání logů ze zařízení	Splňuje (ANO/NE)
Apache httpd	ANO
Apache Tomcat	ANO
Amavis	ANO
Antivir AVG	ANO
Antivir Avast	ANO
Antivir Eset	ANO
Antivir Eset Remote administrator	ANO
Brocade FC switches	ANO
ArcSight CEF format all sources	ANO
Cisco ASA	ANO
Cisco Firepower	ANO
Cisco IOS	ANO
Cisco IronPort	ANO
Cisco SMB	ANO
Cisco WLC	ANO
Dell iDrac (Server OoB management)	ANO
Dell PowerConnect	ANO
FlowMon	ANO
FortiGate (FOS 5.2)	ANO
FreeRADIUS	ANO
Qradar LEEF format all sources	ANO
HPE iLo 4 (Server OoB management)	ANO
HPE switches Procurve OS	ANO
HPE switches Comware OS	ANO
CheckPoint	ANO
JSON (format)	ANO
Kaspersky Endpoint Security	ANO
Kaspersky Security Center	ANO
Kerio Connect	ANO

Kerio Control	ANO
Linux Cron	ANO
Linux Freeradius	ANO
Linux Iptables	ANO
Linux postfix	ANO
LOGmanager	ANO
Mikrotik	ANO
Microsoft Exchange log	ANO
Microsoft SharePoint	ANO
Microsoft SQL	ANO
Microsoft Windows DHCP log	ANO
Microsoft Windows firewall	ANO
Microsoft Windows IIS	ANO
MySQL	ANO
Nginx	ANO
OpenSSH server	ANO
Oracle DB	ANO
PostgreSQL	ANO
Sophos	ANO
SpamAssasin	ANO
Synology NAS DSM	ANO
VMware	ANO
Windows - any logs from Event Viewer	ANO
Windows - any text log from file	ANO