

KUPNÍ SMLOUVA

uzavřená podle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
(dále jen „občanský zákoník“)

Číslo smlouvy Kupujícího: ČÚZK-060858/2024

Číslo smlouvy Prodávajícího:

Smluvní strany

Kupující: **ČR-Český úřad zeměměřický a katastrální**

Se sídlem: Pod sídlištěm 1800/9, 182 11 Praha 8

Jejíž jménem jedná: Ing. Radek Chromý, Ph.D., místopředseda

IČO: 00025712

ID DS: uuaaatg

(dále jen „Kupující“)

a

Prodávající: **T-SOFT a.s.**

Se sídlem: Za Brumlovkou 1559/5 Praha 4

Zastoupená: Ing. Michalem Vaněčkem, Ph.D., MBA,
místopředsedou představenstva

Zapsaná: do obchodního rejstříku vedeného Městským soudem v Praze,
oddíl B, vložka 15233

IČO: 40766314

DIČ: CZ40766314

ID DS: vrugr8f

(dále jen „Prodávající“)

uzavírají níže uvedeného dne kupní smlouvu za níže uvedených podmínek.

1 Předmět plnění

1. Předmětem této kupní smlouvy (dále jen „Smlouva“) je nákup logovacího systému pro bezpečnostní monitoring pro rezort Kupujícího, Prodávající se tedy zavazuje k dodání

zařízení, jejichž přesná specifikace včetně souvisejících služeb je uvedena v Příloze č. 1 této Smlouvy (dále jen „plnění“), to vše v rozsahu a za podmínek uvedených v této Smlouvě, jejích přílohách, zadávací dokumentaci k veřejné zakázce „Infrastruktura pro uchování logů bezpečnostního monitoringu“ a nabídce Prodávajícího předložené v rámci této veřejné zakázky.

2. Kupující se tímto zavazuje za podmínek stanovených touto Smlouvou plnění včetně průvodních dokladů převzít a zaplatit za ně Prodávajícímu kupní cenu stanovenou v této Smlouvě.
3. Plnění bude Prodávající provádět na profesionální úrovni v kvalitě odpovídající všeobecně uznávaným standardům pro daný okruh činností.
4. Obsahem tohoto závazkového vztahu jsou všechny podmínky, práva a povinnosti stanovené v zadávací dokumentaci a jejích přílohách a nabídce Prodávajícího i v případě, že nejsou touto Smlouvou výslovně uvedeny.
5. Smluvní strany prohlašují, že tuto Smlouvu, jakož i jednotlivá práva a povinnosti z ní vyplývající, budou vykládat v souladu se zadávacími podmínkami VZ a nabídkou Prodávajícího předloženou v rámci tohoto zadávacího řízení.
6. Dodávané plnění, resp. všechny jeho komponenty budou nové.
7. Součástí plnění je potvrzení výrobce (nebo jeho zastoupení) o určení dodávaného plnění pro evropský trh).
8. Prodávající odpovídá za to, že poskytnuté plnění bude ke dni předání splňovat funkční specifikaci stanovenou zadávací dokumentací, jeho nabídkou do zadávacího řízení a Smlouvou, bude implementováno a provozuschopné v prostředí Kupujícího a bude mít příslušnou dokumentaci.
9. Prodávající se zavazuje zajistit, že pro poskytování plnění dle Smlouvy budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví.
10. Pro realizaci plnění má Prodávající právo použít smluvní poddodavatele. Seznam poddodavatelů předložil Prodávající před podpisem této Smlouvy. Prodávající má právo použít k plnění i další poddodavatele po předchozím odsouhlasení Kupujícím. Kupující odsouhlasení nového poddodavatele bezdůvodně neodmítne. V případě, že Prodávající využívá poddodavatele k výkonu činností vymezených v této Smlouvě, odpovídá za kvalitu, bezpečnost a včasnost plnění stejným způsobem, jako by činnost prováděl sám.
11. V případě, že Prodávající využívá poddodavatele k výkonu činností definovaných touto Smlouvou, je povinen informovat poddodavatele o požadavcích na bezpečnost informací a bezpečnostních pravidlech, které je povinen dodržovat při výkonu dané činnosti alespoň ve stejném rozsahu, v jakém to Kupující požaduje od Prodávajícího.
12. Prodávající deklaruje, že osoby a/nebo případně poddodavatelé, jejichž odbornou kvalifikací bylo prokázáno v jeho nabídce na veřejnou zakázku splnění technických kvalifikačních předpokladů, budou skutečně zapojeny do plnění předmětu Smlouvy, a to minimálně do akceptace plnění. V případě nutné změny těchto osob a/nebo poddodavatelů z důvodů Prodávajícího musí Prodávající doložit splnění srovnatelných kvalifikačních předpokladů pro nové osoby a/nebo poddodavatele. Po dobu, kdy Prodávající neplní tento

svůj závazek, je v prodlení s poskytováním plnění dle této Smlouvy a Kupující má právo požadovat slevu z celkové ceny plnění ve výši 0,2 % za každý den takového prodlení.

13. Uplatní-li třetí osoba vůči Kupujícímu před soudem nebo mimo soud jakékoli své nároky k plnění či jeho části (zejména v oblasti práv duševního vlastnictví, jako například patentových a autorských práv a obchodních značek) Prodávající bude Kupujícího před těmito nároky bránit a důvodné nároky třetí osoby na vlastní náklady bez zbytečného odkladu vypořádá, případně poskytne na vlastní náklady právní servis/zastupování v obvyklé výši pro Kupujícího při jeho obraně. Vypořádání, právní servis/zastupování bude poskytnuto v případě, že Prodávající bude neprodleně písemně informován Kupujícím o nároku uplatněném třetí stranou a budou mu ze strany Kupujícího poskytnuty potřebné informace a součinnost. Prodávající se také zavazuje v této souvislosti uhradit případné veškeré škody, pokuty, náklady apod., které bude Kupující povinen v důsledku výše uvedeného uhradit.
14. Prodávající bere na vědomí, že plnění může být a bude používáno i dalšími organizačními složkami státu (OSS) z resortu Kupujícího, tj. ČR-Zeměměřickým úřadem, zeměměřickými a katastrálními inspektoráty a katastrálními úřady.
15. Prodávající je povinen Kupujícímu předem informovat o významné změně ovládnutí Prodávajícího. Ovládnutím se zde rozumí zejména ovládnutí či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, či ekvivalentní postavení. Notifikační povinnost je také navázána na změnu skutečného majitele v evidenci skutečných majitelů (§ 118b a násl. zákona č. 304/2013 Sb., o veřejných rejstřících právnických a fyzických osob a o evidenci svěřenských fondů). Kupující je povinen bez zbytečného odkladu sdělit své stanovisko ohledně svého záměru dále pokračovat či nepokračovat ve smluvním vztahu založeném touto Smlouvou i po změně ovládnutí Prodávajícího.
16. Kupující v souladu s ustanovením § 6 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, trvá na dodržování zásady sociálně odpovědného zadávání, environmentálně odpovědného zadávání a inovací ve smyslu daného zákona. S ohledem na charakter zakázky Kupující zejména požaduje po Prodávajícím, aby v průběhu plnění této Smlouvy dodržoval a zajistil dodržování pracovněprávních předpisů (zejména zákoníku práce a zákona o zaměstnanosti) vůči všem osobám, které se na plnění této Smlouvy budou podílet. Prodávající se zavazuje, že bude dodržovat veškeré povinnosti vyplývající z právních předpisů České republiky, zejména pak z předpisů pracovněprávních, předpisů z oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod., a to vůči všem osobám, které se na plnění veřejné zakázky podílejí, a to včetně poddodavatelů; a v případě požadavku Kupujícího mu dodržování daných povinností doloží. Prodávající je také povinen využít u použitých obalů recyklovatelný materiál, nebo materiál z obnovitelných zdrojů, nebo obalový systém pro opakované použití a zajistit ekologickou likvidaci případného elektro a ostatního odpadu (včetně veškerého odpadu po pracích souvisejících s plněním záruky).

2 Licenční ujednání

1. Součástí plnění může být tzv. proprietární software, a/nebo tzv. open source software, který naplňuje znaky díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „autorský zákon“). V této souvislosti pak poskytuje Prodávající Kupujícímu nevýhradní oprávnění k výkonu práva autorské dílo užít (dále jen „licenci“) pro potřeby resortu Kupujícího nejméně po dobu trvání této Smlouvy na území

České republiky, a to všemi způsoby a v množstevním rozsahu nezbytném pro naplnění účelu této Smlouvy v souladu se zadávacími podmínkami. Kupující není povinen licenci využít.

2. Prodávající je povinen zajistit pro Kupujícího licenci takovým způsobem, aby mohl být naplněn účel této Smlouvy a byla dodržena všechna licenční ujednání k dílu a všechny právní předpisy upravující jeho užití, a to alespoň v rozsahu nezbytném pro naplnění účelu Smlouvy.
3. Prodávající prohlašuje, že užitím díla Kupujícím nebudou neoprávněně porušena žádná práva a oprávněné zájmy třetích osob, kromě práv duševního vlastnictví také např. právo na ochranu osobnosti fyzických osob a právo na ochranu dobré pověsti právnických osob.
4. Prodávající se zavazuje, že jakákoli dodaná nebo zpřístupněná aktualizace, nebo jiná úprava je autorskoprávně nezávadná dle této Smlouvy a podléhá stejné licenci, jako je uvedena v této Smlouvě.
5. Prodávající se zavazuje zajistit služby podpory (maintenance) k licencím v dostatečném rozsahu, je-li to pro naplnění účelu Smlouvy nezbytné, resp. vyžadují-li to licenční či jiné podmínky použití tohoto SW.
6. Odměna za veškerá oprávnění poskytnutá Kupujícímu dle této Smlouvy je již zahrnuta v ceně plnění dle této Smlouvy. Cena plnění obsahuje všechny licenční odměny, které mohou při plnění z této Smlouvy vzniknout. Prodávající není oprávněn uplatňovat další licenční poplatky s ohledem na způsob použití licencí a charakteristiku prostředí, ve kterém jsou užívány. V ceně plnění dle této Smlouvy je zahrnuta i cena případně poskytnutých služeb podpory k SW, či jiných souvisejících plnění, se kterými jsou spojeny jednorázové či pravidelné poplatky, za celou dobu trvání Smlouvy. Smluvní strany mají za to, že je tímto odměna za licence ujednána, resp. je sjednán způsob jejího určení dostatečným způsobem s ohledem na ustanovení § 2366 občanského zákoníku.
7. Prodávající touto Smlouvou poskytuje Kupujícímu licenci k dílu, přičemž účinnost této licence nastává okamžikem podepsání akceptačního protokolu s výsledkem „akceptováno“; do té doby je Kupující oprávněn dílo užít v rozsahu a způsobem nezbytným k naplnění účelu této Smlouvy.
8. Licenční podmínky uvedené v příloze Smlouvy nesmí být v rozporu s účelem této Smlouvy a pro odstranění veškerých pochybností se nepoužijí takové licenční podmínky uvedené v příloze Smlouvy, které jsou v rozporu s účelem a textem této Smlouvy.

3 Dodací podmínky

1. Prodávající je povinen dodat plnění v množství a jakosti a v provedení dle této Smlouvy.
2. Kupující požaduje dodání plnění do 90 dní ode dne nabytí účinnosti Smlouvy.
3. Záruční podpora a nadstandardní podpora bude poskytována po dobu 60 měsíců akceptace plnění.
4. Záruka za jakost/záruka na funkčnost SW bude poskytována po dobu 60 měsíců od data podepsání akceptačního protokolu s výsledkem „akceptováno“. Pokud je akceptační řízení ukončeno akceptací s výhradou, tak záruční doba počíná běžet až po odstranění vad.

5. Místem plnění této veřejné zakázky je sídlo Kupujícího a datové centrum umístěné v Praze.
6. Vlastnické právo k hmotným součástem plnění přechází na Kupujícího podepsáním akceptačního protokolu s výsledkem „akceptováno“. Pokud je akceptační řízení ukončeno akceptací s výhradou, tak vlastnictví přejde až po odstranění vad. Nebezpečí škody na hmotných součástech plnění (či jeho dílčí části) přejde z Prodávajícího na Kupujícího dnem protokolárního převzetí hmotných součástí plnění (či jeho dílčí části) a Kupujícímu zároveň vznikne právo hmotné součásti plnění (či jeho dílčí části) užívat v souladu s účelem této Smlouvy.

4 Komunikace, kontaktní osoby, součinnost

1. Veškerá komunikace Kupujícího s Prodávajícím v průběhu plnění Smlouvy bude probíhat v českém nebo slovenském jazyce.
2. Každá ze smluvních stran jmenuje osobu oprávněnou ve věcech smluvních, tedy především k předání a převzetí plnění, k objednání plnění a k podepisování akceptačních protokolů:

Za Kupujícího:

Za Prodávajícího:

3. Každá ze smluvních stran jmenuje kontaktní osobu ve věcech technických:

Za Kupujícího:

Za Prodávajícího:

4. Smluvní strany jsou oprávněny jednostranně změnit výše uvedené osoby, jsou však povinny na takovou změnu druhou stranu písemně předem upozornit.
5. Pokud se mezi smluvními stranami předpokládá písemný kontakt, je za písemný projev považován zpráva zaslaná prostřednictvím datových schránek, dopis, příp. e-mailová zpráva s dokladem o tom, že byla druhé smluvní straně doručena.
6. Smluvní strany se zavazují úzce spolupracovat, zejména si poskytovat úplné, pravdivé, včasné informace a dohodnuté podmínky a součinnost umožňující řádné plnění Smlouvy.
7. V zájmu plnění Smlouvy jsou smluvní strany povinny plnit řádně a včas své závazky tak, aby nedocházelo k prodlení s jejich plněním.

5 Akceptační řízení

1. Akceptační řízení bude zahájeno výzvou Prodávajícího k provedení akceptačního řízení (po předání předmětu plnění včetně příslušné dokumentace a instalaci v požadovaném

rozsahu), tak aby bylo možno na straně Kupujícího ověřit funkčnost dodaného plnění, provést akceptační testy a dokumentovat případné zjištěné nedostatky.

2. Při akceptačním řízení budou projednány výhrady Kupujícího, stanovena jejich výsledná závažnost, určen způsob a termín jejich odstranění.
3. Vadou se rozumí rozpor mezi skutečnými funkčními vlastnostmi poskytnutého plnění a funkčními vlastnostmi, které jsou stanoveny v příslušných dokumentacích a nabídce Prodávajícího. Za vadu se považuje i skutečnost, že funkční vlastnosti poskytnutého plnění neodpovídají požadovaným minimálním základním požadavkům, viz Příloha 1 Smlouvy – „Podrobná technická specifikace plnění“. Za vadu se považuje i skutečnost, že funkční vlastnosti poskytnutého plnění neodpovídají povinným funkčním vlastnostem, jak vyplývají z technických norem, pokud se takové technické normy na plnění vztahují a jsou vůči němu závazné. Za vadu se dále považují i právní vady plnění.
4. Předmět plnění se považuje za předaný, potvrdí-li Kupující podpisem v akceptačním protokolu, že předmět plnění přebírá bez výhrad, případně s výhradami (viz níže). Součástí akceptačního protokolu bude záznam o předání plnění včetně dokumentace.
5. Akceptační řízení musí být ukončeno nejpozději do 7 pracovních dnů od jeho zahájení.
6. Možné výsledky akceptačního řízení

- *Akceptováno*

V případě, že Kupující v průběhu akceptačního řízení nenalezne v předaném plnění žádné vady ani nedodělky, uvede Kupující do akceptačního protokolu, že předané plnění přebírá bez výhrad a obě strany akceptační protokol potvrdí svým podpisem.

Výsledky plnění budou akceptovány v případě, že dodané plnění bude funkční a bude splňovat funkční specifikaci stanovenou zadávacími podmínkami a nabídkou Prodávajícího a plnění bude mít řádnou dokumentaci.

V případě akceptace je Prodávající oprávněn fakturovat cenu dodávky logovacího systému.

- *Akceptováno s výhradou*

Pokud bude plnění obsahovat malé vady, které nebudou bránit provoznímu nasazení, pak Kupující připouští „akceptaci s výhradou“. V tomto případě musí být vady uvedeny v akceptačním protokolu a stanoven termín odstranění vad. Součástí odzkoušení vad je i aktualizace dokumentací. Po vystavení akceptačního protokolu s výhradou je možno fakturovat 80% z ceny dodávky logovacího systému. Po odstranění všech vad a podepsání protokolu o odstranění těchto vad zbývajících 20% této ceny dodávky logovacího systému.

- *Neakceptováno*

V případě, že budou v průběhu akceptačního řízení v předaném plnění zjištěny vady a nedodělky, které by bránily v užití plnění či jeho části, respektive plnění neodpovídá podmínkám nezbytným pro akceptaci uvedeným výše, není předané plnění akceptováno. Obě strany se dohodnou na termínech nového předání a nového akceptačního řízení. Do akceptačního protokolu Kupující uvede, že předané plnění nebylo akceptováno, popíše vady a nedodělky, případně požadavky na dopracování, termíny nového předání a akceptačního řízení a obě strany akceptační protokol potvrdí svým podpisem. V tomto případě je Prodávající v prodlení s předáním plnění a Kupující uplatní sankce z prodlení.

Doba prodlení s plněním se přitom počítá od smluvního termínu splnění (případná nesoučinnost Kupujícího se do doby prodlení Prodávajícího nezapočítává). Při neakceptaci předmětu plnění nevzniká Prodávajícími právo fakturovat.

6 Platební podmínky

1. Kupní cena byla sjednána dohodou smluvních stran a činí:

Číslo položky	Předmět plnění podle kapitoly 3 ZD	Jednotka	Cena za jednotku bez DPH	Počet jednotek	Celková cena bez DPH	Celková cena včetně DPH
1.	Dodávka logovacího systému včetně všech požadovaných služeb a záruky za jakost/záruky na funkčnost SW v prvních dvou letech	kus	2 532 900	1	2 532 900	3 064 809
2.	Záruka za jakost/záruka na funkčnost SW 3. až 5. rok	čtvrtletí	70 925	12	851 100	1 029 831
3	Nadstandardní podpora	MD	10 000	80	800 000	968 000
4.	Celková cena předmětu plnění	--	---	---	4 184 000	5 062 640

- Cena plnění zahrnuje veškeré náklady Prodávajícího nutné k poskytnutí plnění, jakož i veškeré náklady související. Prodávající prohlašuje, že před podpisem této Smlouvy, důkladně prošel zadávací dokumentaci, zvážil všechny varianty možného způsobu plnění zakázky a na základě těchto informací stanovil cenu plnění uvedenou do nabídky. Tato cena je maximální a nepřekročitelná (s výjimkou změny sazby DPH) a Prodávající je povinen za tuto cenu plnění dokončit tak, aby bylo dosaženo účelu a předmětu této Smlouvy, a to i v případě, že by se v průběhu plnění Smlouvy zjistilo, že ke splnění účelu a předmětu této Smlouvy je nutné vynaložit další náklady nebo zvolit jiné postupy.
- Smluvní strany se dohodly na bezhotovostním placení na účet Prodávajícího dle pravidel uvedených v této Smlouvě.
- Cena za dodávku logovacího systému bude uhrazena po akceptaci předmětu plnění. Faktura musí být označena registračním číslem projektu CZ.06.01.01/00/22_005/0002279, ze kterého bude předmět plnění částečně financován.
- Cena za záruku za jakost/záruku na funkčnost SW za 3. až 5. rok bude hrazena Prodávajícímu čtvrtletně zpětně.

6. Cena za nadstandardní podporu bude uhrazena na základě akceptačního protokolu předmětného plnění objednaného v rámci nadstandardní podpory.
7. Vystavená faktura bude mít náležitosti stanovené zákonem o DPH č. 235/2004 Sb., v platném znění a termín splatnosti 21 dnů po doručení Kupujícímu. Povinnost zaplatit je splněna dnem odepsání příslušné finanční částky z bankovního účtu Kupujícího na účet Prodávajícího, není-li smluvními stranami sjednáno jinak. Faktura může být zaslána elektronicky na cuzk@cuzk.cz
8. Nebude-li vystavená faktura obsahovat náležitosti uvedené v předchozích ustanoveních nebo bude chybně vyúčtována cena, bude taková faktura do data splatnosti Prodávajícímu vrácena k doplnění scházejících údajů nebo k opravě nesprávných údajů. Prodávající provede opravu vystavením nové faktury s novou dobou splatnosti, která nesmí být co do počtu dnů kratší než doba splatnosti původní faktury. Bude-li vadná faktura vrácena, přestává běžet původní doba splatnosti. V takovém případě nedojde k prodlení s placením. Celá doba splatnosti běží znovu ode dne doručení nově vystavené faktury na konkrétní fakturační místo.

7 Podmínky požadované záruky za jakost/ záruky na funkčnost SW (společně dále „záruka“)

1. Dodané plnění bude po dobu 60 měsíců způsobilé k obvyklému použití pro stanovený účel a zachová si obvyklé vlastnosti.
2. Počátek běhu doby záruky je stanoven na den následující po dni podepsání akceptačního protokolu s výsledkem „akceptováno“. Pokud je akceptační řízení ukončeno akceptací s výhradou, tak doba záruky počíná běžet až po odstranění vad.
3. Hlášení závad bude probíhat na jediné objednávkové místo servisních zásahů pro všechny technické komponenty.
4. Zajištění komunikace v českém (případně slovenském) jazyce.
5. Záruční podpora bude poskytována v pracovní dny od 8:00 do 16:00 na Prodávajícím definované kontaktní místo (telefon, email, webové rozhraní).
6. Prodávající je povinen plně hradit veškeré náklady záruky, s výjimkou nákladů na zásahy vyvolané neodbornou manipulací na straně pracovníků Kupujícího, a nákladů na zbytečný výjezd pracovníků Prodávajícího.
7. Plnění ze záruky bude poskytnuto pro všechny části dodaného HW a všechny jejich dílčí komponenty.
8. Prodávající se zavazuje k obnovení provozuschopnosti plnění do konce následujícího pracovního dne po nahlášení závady (SLA NBD fix time on-site). Provozuschopností se tímto myslí obnovení celého zařízení do provozuschopného stavu, na který bude následně nahrána poslední záloha konfigurace.
9. Prodávající se zavazuje k přednostnímu provádění zásahu v místě instalace dodávaného HW. V případě výskytu závady, jejíž odstranění z jakýchkoli důvodů nebude na místě možné, je Prodávající povinen Kupujícímu bezplatně poskytnout nový náhradní HW (popřípadě náhradní díl) v konfiguraci nejméně stejně funkční jako vadný HW (díl), tak aby Kupující mohl řádně užívat plnění bez omezení do doby, než bude odstraněna vada. Jestliže dojde k opravě, bude původní HW (díl) po opravě navrácen. Veškerá manipulace

s HW bude protokolárně zaznamenána. V případě, že oprava vadné komponenty nebude možná, bude předmětná komponenta nahrazena novou stejných nebo lepších parametrů.

10. Prodávající musí při manipulaci s HW (výměna HW, či dílu) zajistit, aby pevné disky, které obsahují již zaznamenané logy, zůstaly v prostředí Kupujícího. Pokud bude závada na pevném disku, je Prodávající povinen se řídit interními předpisy Kupujícího, se kterými bude Prodávající seznámen po podpisu Smlouvy.
11. Prodávající poskytne Kupujícímu ve vztahu k SW právo na aktualizace SW zdarma minimálně 4x ročně a záruku na funkčnost po stanovenou dobu. Podpora musí obsahovat telefonickou a emailovou podporu s diagnostikou vzdáleným přístupem.

8 Podmínky požadované nadstandardní podpory

1. Nadstandardní podpora bude čerpána na základě požadavků Objednatele.
2. Nadstandardní podpora bude čerpána do maximálního rozsahu 80 MD, přičemž maximální rozsah nemusí být vyčerpán.
3. Předmětem nadstandardní podpory bude zejména nastavení bezpečnostního monitoringu ze všech infrastrukturních prvků, aplikací a od všech uživatelů, definovaných dle usecase pro zvyšování bezpečnosti resortu.
4. Kupující zašle mailem Prodávajícímu svůj problém, který uvažuje řešit v rámci nadstandardní podpory. K tomu Prodávající do 5 pracovních dnů zašle zpět Kupujícímu návrhy variant řešení, včetně maximální doby implementace každé varianty řešení, která se počítá ode dne objednání nadstandardní podpory a závazně vyčíslí maximální počet MD pro každou z uvedených variant řešení.
5. Kupující zváží návrhy řešení předložené Prodávajícím a v případě rozhodnutí implementace jedné z variant řešení zašle Prodávajícímu objednávku na zajištění nadstandardní podpory s termínem implementace, který nebude kratší než v návrhu řešení uvedená doba implementace. Písemná objednávka bude podepsána kontaktní osobou ve věcech smluvních. Prodávající potvrdí Kupujícímu doručitou objednávku nejpozději 2. pracovní den, následující po dni, kdy byla odeslána objednávka. Následně Prodávající zahájí plnění služby v režimu nadstandardní podpory.

9 Sankční podmínky

1. V případě prodloužení Kupujícího s úhradou plateb sjednaných v této Smlouvě, je Prodávající po Kupujícím oprávněn požadovat uhrazení smluvní pokuty ve výši 0,05 % z dlužné částky za každý započatý den prodloužení.
2. V případě prodloužení s předáním plnění nebo jeho součástí bude Kupující požadovat po Prodávajícím slevu z ceny ve výši 0,2% z celkové ceny dodávky logovacího systému bez DPH za každý započatý den prodloužení.
3. V případě prodloužení s odstraněním vady je Prodávající povinen poskytnout Kupujícímu slevu z ceny ve výši 500 Kč za každý započatý pracovní den prodloužení.

4. V případě prodlení s odstraněním vad stanovených v akceptačním protokolu v případě akceptace s výhradou je povinen Prodávající poskytnout slevu z ceny ve výši 2 000 Kč za každý započatý pracovní den prodlení a za každou uvedenou vadu.
5. V případě nesplnění termínu implementace plnění objednaného v rámci nadstandardní podpory bude Objednatel požadovat po Dodavateli slevu z ceny ve výši 0,2 % z ceny tohoto plnění v Kč bez DPH za každý započatý pracovní den prodlení Dodavatele.
6. Za porušení povinnosti mlčenlivosti je porušující smluvní strana povinna uhradit druhé smluvní straně pokutu ve výši 100 000 Kč, a to za každý jednotlivý případ porušení povinnosti. Právo vymáhat a účtovat smluvní pokutu za porušení povinnosti mlčenlivosti vzniká oprávněné smluvní straně prvním dnem následujícím po doručení oznámení o prokazatelném porušení povinnosti mlčenlivosti smluvní stranou.
7. Sleva z ceny bude poskytnuta v rámci fakturace bezprostředně následující po porušení povinnosti Prodávajícího.
8. Poskytnutí slevy z ceny či smluvní pokuty nezbavuje povinnou smluvní stranu povinnosti splnit své závazky.
9. Každá ze smluvních stran je oprávněna požadovat náhradu škody i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje sleva z ceny či smluvní pokuta, a to v celém rozsahu. Odstoupením od smlouvy nárok na slevu z ceny či smluvní pokutu nezaniká.

10 Povinnost mlčenlivosti

1. Za důvěrné informace se bez ohledu na formu jejich zachycení považují ty informace, které jedna ze smluvních stran výslovně označila za důvěrné (dále jen „Důvěrné informace“).
2. Kupující považuje mimo jiné za důvěrné veškeré technické informace o jeho vnitřním prostředí a technické detaily týkající se technické infrastruktury, které nejsou obecně známy.
3. Smluvní strany se zavazují, že během plnění Smlouvy i po jejím ukončení budou chránit Důvěrné informace druhé smluvní strany, o kterých se dozví od druhé smluvní strany v souvislosti s plněním Smlouvy, tak, jako chrání svoje vlastní informace stejné důležitosti a budou ve vztahu k nim zachovávat mlčenlivost a nepřístupní je třetí osobě. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, o povinnosti mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zajistit dodržování těchto povinností všemi osobami podílejícími se na plnění této Smlouvy.
4. Za třetí osoby se ve smyslu této Smlouvy nepovažují:
 - zaměstnanci smluvních stran a osoby v obdobném postavení,
 - poddodavatelé druhé smluvní strany za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny smluvním stranám v této Smlouvě.

5. Bez ohledu na výše uvedená ustanovení se za Důvěrné informace nepovažují informace, které:
- se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení povinnosti druhé smluvní strany či právních předpisů;
 - měla druhá smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi smluvními stranami uzavřené smlouvy;
 - po podpisu této Smlouvy poskytne druhé smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi;
 - je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU nebo závazným rozhodnutím oprávněného orgánu veřejné moci;
 - jsou obsažené ve Smlouvě (ledaže podléhají výjimce z uveřejnění podle příslušných právních předpisů) anebo jsou zveřejněné na příslušných webových stránkách dle platné právní úpravy;
 - které jsou poskytnuty se souhlasem druhé smluvní strany.
6. Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající smluvní strany a přijímající smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní Důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě smluvní strany zavazují neduplikovat žádným způsobem Důvěrné informace druhé smluvní strany, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Smluvní strany se zároveň zavazují nepoužít Důvěrné informace druhé smluvní strany jinak než za účelem plnění této Smlouvy.
7. Veškerá data a provozní údaje zůstávají výhradním vlastnictvím Kupujícího, Prodávající je s nimi oprávněn nakládat pouze v nezbytně nutném rozsahu, tj. neduplikovat je žádným způsobem, nepředat je třetí osobě ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu, a to pouze po nezbytně dlouhou dobu. Veškerá data, provozní údaje, přihlašovací údaje apod. musí být Prodávajícím zlikvidována nejpozději s ukončením Smlouvy.

11 Povinnosti vztahující se ke kyberbezpečnosti

1. Prodávající je dále povinen dodržovat bezpečnostní politiku Kupujícího, byl-li s ní seznámen.
2. Kupující bere na vědomí, že postup zvládnutí kybernetického bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Kupujícího, nebude posuzován jako okolnost vylučující odpovědnost Kupujícího za prodlení s řádným a včasným plněním Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Kupujícího či jiné osobě ze strany Prodávajícího. Ostatní ustanovení ohledně odpovědnosti Prodávajícího za prodlení obsažená ve Smlouvě nejsou tímto ustanovením dotčena.
3. Kupující po dobu plnění této Smlouvy umožní Prodávajícímu přístup prostřednictvím VPN řízený přístup k produkčnímu prostředí souvisejícím s plněním Smlouvy.
4. Přístup k produkčnímu prostředí bude Prodávající využívat v minimálně nutném rozsahu pro naplnění účelu Smlouvy.

12 Odstoupení od Smlouvy

1. Strany jsou oprávněny od Smlouvy odstoupit pouze v případě závažného porušení smluvní nebo zákonné povinnosti protistranou (tzv. podstatné porušení povinnosti) a dále v případech výslovně vymezených touto Smlouvou.
2. Za podstatné porušení povinnosti ze strany Prodávajícího se považuje zejména zpoždění s řádným plněním dle Smlouvy (zejména pozdní dodání, nedodržení SLA atd.) delším než 15 pracovních dní.
3. Obě smluvní strany mají právo odstoupit od Smlouvy v případě, že okolnosti vyšší moci trvají déle než 3 měsíce.
4. Kupující je oprávněn odstoupit od této Smlouvy v případě významné změny kontroly Prodávajícího s tím, že změnou kontroly Prodávajícího se rozumí změna ovládání či řízení podle § 74 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, změna vlastnictví zásadních aktiv, popřípadě změna oprávnění nakládat s těmito aktivy, využívanými Prodávajícím k plnění Smlouvy.
5. Účinky každého odstoupení od Smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této Smlouvy druhé smluvní straně. Odstoupením od Smlouvy nezaniká nárok na náhradu škody vzniklé porušením Smlouvy ani oprávněného nároku na zaplacení smluvních pokut resp. poskytnutí slev z cen.
6. Ukončením účinnosti této Smlouvy nejsou dotčena ustanovení Smlouvy o mlčenlivosti a ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této Smlouvy.

13 Vyšší moc

1. Žádná ze smluvních stran nebude považována za odpovědnou za nesplnění některého ustanovení této Smlouvy, budou-li příčinou nepředvídatelné, neodvratitelné a povinnou stranou nekontrolovatelné okolnosti nebo události, která způsobují, že plnění povinností není možné nebo je krajně obtížné. Za vyšší moc se považují zejména epidemie, ozbrojené konflikty, přírodní katastrofy, meteorologické podmínky apod., a to pouze za podmínky, že splňují požadavky v předchozí větě (dále též jako „vyšší moc“).
2. Smluvní strana, která porušuje svou povinnost nebo která s přihlédnutím ke všem okolnostem má vědět, že poruší svou povinnost založenou touto Smlouvou, nebo která se dozví o okolnosti vyšší moci, bránící plnění povinnosti dle této Smlouvy, je povinna oznámit písemně druhé smluvní straně povahu překážky, která jí brání nebo bude bránit v plnění povinnosti, a o jejích důsledcích. Zpráva musí být podána bez zbytečného odkladu, nejpozději však do 5 pracovních dnů poté, kdy se povinná smluvní strana o překážce dověděla nebo při náležité péči mohla dovědět. Druhá smluvní strana je povinna přijetí takové zprávy bez zbytečného odkladu písemně potvrdit. Stejným způsobem musí být obeznamena druhá smluvní strana o ukončení okolností bránících splnění povinností vyplývajících z této Smlouvy.

14 Závěrečná ujednání

1. Tato Smlouva se řídí právním řádem České republiky. Vztahy mezi smluvními stranami se řídí zejména občanským zákoníkem, pokud Smlouva nestanoví jinak.

2. Tuto Smlouvu je možné měnit pouze písemnou dohodou smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných za každou smluvní stranu osobou nebo osobami oprávněnými jednat jménem smluvních stran, a to předchozím řádném projednání Smluvními stranami.
3. Pro případy promlčení se použije úprava obsažená v občanském zákoníku.
4. Spory vyplývající z této Smlouvy nebo vzniklé v souvislosti s ní nebo vzniklé v souvislosti s plněním mezi Prodávajícím a Kupujícím budou řešeny především dohodou. Pokud k dohodě nedojde, budou spory projednávány před soudy České republiky. V případě řešení sporů před soudem si smluvní strany sjednávají místní příslušnost prvoinstančního soudu podle místa Kupujícího.
5. Smluvní strany berou na vědomí, že tato Smlouva podléhá povinnosti zveřejnění dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv) a nabývá účinnosti nejdříve dnem zveřejnění v registru smluv. Zveřejnění v registru smluv zajistí Kupující.
6. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu včetně účetních dokladů minimálně do 31. 12. 2035. Pokud je v českých právních předpisech stanovena lhůta delší, musí být použita pro úschovu delší lhůta.
7. Prodávající je povinen minimálně do 31. 12. 2035 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (Centra, MMR, MF, Evropské komise, Evropského účetního dvora (dále také „EÚD“), Nejvyššího kontrolního úřadu (dále také „NKÚ“), příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.
8. Obě smluvní strany tímto prohlašují a potvrzují, že veškerá ustanovení a podmínky této Smlouvy byly dohodnuty mezi smluvními stranami svobodně, vážně a určitě, nikoliv v tísní a za nápadně nevýhodných podmínek a na důkaz toho připojují své podpisy.
9. Smlouva nabývá platnosti dnem podpisu oběma smluvními stranami.
10. Nedílnou součástí této Smlouvy jsou přílohy:
 - Příloha č. 1 – Podrobná technická specifikace plnění

Prodávající:

Ing. Michal Vaněček
Digitally signed by
Ing. Michal Vaněček
Date: 2024.09.16
09:02:27 +02'00'

Ing. Michal Vaněček, Ph.D., MBA,
místopředseda představenstva

Kupující:

Radek
Chromý
Podpsal Radek Chromý
DN: cn=Radek Chromý, o=CZ,
o=CR - Český úřad zeměměřický a
katastrální, ou=100067,
email=radek.chromy@czk.cz
Datum: 2024.09.25 09:06:18 +02'00'

Ing. Radek Chromý, Ph.D.
místopředseda ČÚZK

Příloha 1 smlouvy – Podrobná technická specifikace plnění

Identifikace nabízeného logovacího systému: (přesné označení dodávaného HW, identifikace výrobce, part number je-li přidělen, identifikace SW včetně licenčních podmínek apod.)

Předmětem dodávky je hardwarový logovací systém Logmanager XL s rozšířenou diskovou kapacitou. Software Logmanager je součástí boxu včetně licence a rozšířené záruky a podpory hardware i software na 2 roky. Výrobce zařízení: **Logmanager a.s., Zubatého 295/5, 150 00 Praha 5.**

Identifikace dodaných součástí je v následující tabulce:

Produkt	Specifikace	počet	Poznámka
LOGM-XL-HA	Logmanager-XL-druhý a další box v clusteru	1	Box včetně SW vybavení Logmanager, server DELL
LOGM-XL-RNWL-1y-HA	Logmanager-XL SW renewal 1 rok pro druhý a další box v clusteru	2	Rozšířená záruka a podpora 2x 1 rok
LOGM-XL-ADD40TB	Rozšíření diskové kapacity Logmanager-XL a XL-HA na 160 TB	1	

Technická specifikace plnění:

Požadovaný parametr	Nabízená hodnota ¹
1. Systém pracuje jako hardwarová appliance s jedním uceleným webovým rozhraním pro všechny administrátorské i operátorské činnosti. Systém nevyžaduje instalaci dalších systémů a aplikací, vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů.	Zařízení splňuje požadavek. Na následujícím odkazu je ke stažení Logmanager datasheet.. https://logmanager.com/cs/podpora#documents-for-download
2. Možnost zapojení ve vysoké dostupnosti (HA cluster)	Ano, box bude zapojen do HA se stávajícím zařízením. https://doc.logmanager.com/latest/cz/additional-informations/logmanager-with-high-availability/
3. Veškerá konfigurace systému se musí provádět v grafickém rozhraní jednotné uživatelské webové konzole. Systém poskytuje podporu pro vizuální programování pro všechny kroky zpracování strojových dat. Ve webové konzoli se nepřípouští konfigurace za využití skriptů, maker nebo textových konfiguračních polí, do kterých se složité textové skripty/makra vkládají.	Zařízení splňuje požadavek. Konfigurace bude prováděna ve stávajícím rozhraní zařízení, které již Zadavatel provozuje. https://doc.logmanager.com/latest/cz/web-interface/

¹ Zadavatel nepovažuje za dostatečné uvedení hodnoty „ano“ případně „splňuje“ nebo obdobné a požaduje uvedení konkrétních nabízených hodnot.

Požadovaný parametr	Nabízená hodnota ¹
4. Systém umožňuje v grafickém rozhraní vizuálního programovacího jazyka snadno provádět třídění a značkování vstupních dat pro jejich další zpracování. Nepřipouští se nastavování třídění vstupních dat ve formě skriptu/makra zobrazeného v textovém okně.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/ https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/
5. Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: SYSLOG (dle RFC3164, RFC5424, RFC5425) a RELP. Systém musí umožňovat příjem logů i na rozsahu alespoň 50 UDP a TCP portů pro zjednodušené třídění vstupních zpráv. Dále požadujeme podporu sběru strojových dat z databází s nastavením v grafickém menu systému minimálně pro databáze MSSQL, MySQL, Oracle a PostgreSQL, a to bez nutnosti instalovat na databázový server doplňkový software nebo agenta.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager/
6. 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. Integrované parsery systému automaticky přidávají ke zprávám, kterých se to týká, meta informace o jaký druh zprávy se jedná, minimálně požadujeme rozlišení těchto druhů zpráv: úspěšné přihlášení, neúspěšné přihlášení, odhlášení, konfigurační změna, značka/tag. Tyto meta informace musí být možné přidávat i v uživatelsky definovaných parserech.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-log-flow/ https://doc.logmanager.com/latest/cz/web-interface/parser/parsers/
7. Hodnoty jednotlivých parsovaných polí je možné v definici parseru přetypovat a standardizovat alespoň na tyto základní druhy: • číslo, • IP adresa, • MAC adresa, • URL. Nad uloženými čísly je pak možné při prohledávání dat provádět matematické operace (součty všech hodnot, průměry, nejmenší/největší hodnota apod.).	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/parsers/
8. Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, které vzniká v okamžiku přijetí logu systémem a kterým se systém defaultně řídí, případně využívá TSA certifikační razítko.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-log-flow/
9. Všechna pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/search/

Požadovaný parametr	Nabízená hodnota ¹
10. Možnost sběru událostí minimálně ve formátech RAW, Syslog, RFC5424, CEF, LEEF, JSON RFC8259.	Zařízení splňuje požadavek. Viz příložený seznam podporovaných systémů a specifikace: https://logmanager.com/cs/specifikace-produktu
11. Systém nesmí v žádném případě umožnit mazání nebo modifikování již uložených logů v rámci požadované retence. A to ani libovolnou konfigurační změnou – administrátorovi s nejvyššími oprávněními k navrhovanému systému. Každý zpracovaný log musí mít dohledatelný unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.	Zařízení splňuje požadavek. Viz dokumentace: https://logmanager.com/cs/proc-logmanager#security
12. Systém umožňuje konfiguraci filtrace nerelevantních událostí v grafickém rozhraní vizuálního programovacího jazyka. Pro psaní filtrace nesmí být použito textové psaní programového kódu ale tzv. vizuální programování, které automaticky opravuje uživatele a upozorňuje ho na chyby. Předložte odkaz na dokumentaci popisující způsob filtrování nerelevantních událostí.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-filters/
13. Systém provádí konsolidaci logů na interním storage logovacího systému.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/introduction/customer-support/#server-dell
14. Systém umožňuje snadné vyhledávání událostí a okamžité vytváření grafických reportů (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. Reportovací nástroj musí být integrální součástí navrhovaného systému a musí se obsluhovat v jednotném rozhraní nabízeného produktu.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/search/
15. 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 požadované volby automaticky.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/dashboards/
16. Systém umožňuje snadno vytvářet grafické znázornění událostí v dashboardech nad všemi uloženými daty za libovolné časové období bez nutnosti nejprve modifikovat konfiguraci systému nebo parametrů uložených dat. Historická data v požadované délce retence uložená v systému je možné prohledávat okamžitě bez časových prodlev opětovného importu nebo dekomprimace starších dat, prohledávání dat nesmí vyžadovat manuální konfiguraci a zásahy uživatele.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/dashboards/

Požadovaný parametr	Nabízená hodnota ¹
17. Systém podporuje nativní získávání logů z Office365/Microsoft365 prostředí bez ohledu na použitou licenci 365 prostředí a bez nutnosti instalovat dodatečné externí komponenty. Požadujeme předložit link na dokumentaci popisující nastavení systému v jednotném grafickém rozhraní tak, aby získával logy z Office365/Microsoft365.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/sources/office-365/
18. V případě krátkodobého (do 10 minut) až dvouásobného přetížení systému proti jeho tabulkovým hodnotám nesmí dojít ke ztrátě logů nebo nesprávnému stanovení časového razítka. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti.	Zařízení splňuje požadavek. Viz Logmanager Datasheet: https://logmanager.com/cs/podpora/c7efb546-479e-48db-9ea2-c5dfdb7ab12a?do=downloadDocument
19. Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízeními dle normalizovaných polí (uživatelské jméno, zdrojová IP, značka/tag apod.).	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/search/
20. Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. Továrně dodané pohledy na data nesmí jít administrátorem ani uživatelem systému nevratně modifikovat nebo smazat.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/dashboards/
21. Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Pro vytváření nových pohledů na data není přípustné používat povinně SQL jazyk.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/web-interface/logs/reports/
22. Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/dashboards/
23. Na základě pohledu na uložená data lze provést export dat ve strukturovaném formátu tak, jak jsou v továrně nastaveném nebo uživatelsky nastaveném pohledu data skutečně zobrazena.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/
24. Konfigurační a Systémové rozhraní a dokumentace k těmto rozhraním musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce nebo zjednodušená dokumentace odkazující na další dokumentaci v anglickém jazyce, případně na dokumentaci třetích stran.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/
25. Systém nabízí kapacitní i výkonovou škálovatelnost.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/cluster/

Požadovaný parametr	Nabízená hodnota ¹
26. Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 145 TB dat.	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v Logmagager datasheetu ke stažení: https://logmanager.com/cs/podpora#documents-for-download
27. Ze systému je možné za běhu vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.	Zařízení splňuje požadavek. Viz. datasheet produktu: https://logmanager.com/cs/podpora/c7efb546-479e-48db-9ea2-c5dfdb7ab12a?do=downloadDocument
28. Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/
29. Systém obsahuje REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňuje autorizovaný přístup ke strukturované databázi logů.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/logmanager-orchestrator/ https://doc.logmanager.com/3.11.1/web-interface/users/authentication/#technical-support-report-tsr Vzorový návod je připojen na konci tohoto dokumentu.
30. Jednotná centrální webová konzole s jednotným grafickým rozhraním pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa i analýza logů. Není přípustné, aby navrhovaný systém měl více rozdílných konzolí od různých výrobců s rozdílným ovládáním nebo aby se konfigurace musela provádět mimo jednotné webové rozhraní.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/
31. Systém umožňuje jednotné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem na základě typu zdrojů a značek a k jednotlivým ovládacím komponentům systému. Připojte odkaz na dokumentaci popisující vytváření uživatelských rolí v grafickém rozhraní systému.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/users/
32. Dodaný systém musí obsahovat ucelené all-in-one řešení pro parsování a normalizaci přijatých událostí bez nutnosti dodatečné instalace externích aplikací nebo systémů. Jedinou přípustnou výjimkou je monitorování systémů Windows pomocí agentů.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/suggestions-and-tech-tips/how-to-create-a-parsing-rule/ https://doc.logmanager.com/latest/cz/web-interface/parser/
33. Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření lokálního účtu. Systém automaticky zaznamenává uživatelská jména u akcí provedených konkrétním uživatelem.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/users/ldap-groups/

Požadovaný parametr	Nabízená hodnota ¹
Minimální HW parametry požadovaného systému	
1. Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely.	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v Logmagager datasheetu ke stažení: https://logmanager.com/cs/podpora#documents-for-download
2. HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) pro svoji činnost a je nezávislá na dalších systémech.	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v Logmagager datasheetu ke stažení: https://logmanager.com/cs/podpora#documents-for-download
3. Minimálně 4x 10Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. Konfigurace všech parametrů síťového rozhraní včetně link agregace dle LACP (802.3ad), VLAN a IP adresace v jednotném webovém rozhraní systému.	Zařízení splňuje požadavek. Viz dokumentace a datasheet: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/logmanager-orchestrator/ https://logmanager.com/cs/podpora/c7efb546-479e-48db-9ea2-c5dfdb7ab12a?do=downloadDocument
4. Ventilátory v systému musí být vyměnitelné za provozu a redundantní.	Zařízení splňuje požadavek, jsou použity 6x DELL High Performance Fanš.
5. 2x napájecí zdroje s redundancí napájení 1+1.	Zařízení splňuje požadavek, jsou použity DELL Dual, Hot-Plug, Power Supply, 1100W MM (100-240Vac) Titanium, Redundant (1+1).
6. Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-system-server-management/
7. Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdobu HP iLO, Dell iDRAC apod).	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-system-server-management/
Výkonnostní a SW parametry systému	
1. Systém funguje formou HW appliance (všechny části systému je možné nastavit v centrální webové konzoli a není nutné editovat žádné konfigurační soubory, scripty nebo makra v příkazové řádce).	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v Logmagager datasheetu ke stažení: https://logmanager.com/cs/podpora#documents-for-download dále viz manuál: https://doc.logmanager.com/latest/cz/web-interface/system/

Požadovaný parametr	Nabízená hodnota ¹
2. Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna uživatelsky přes centrální webovou správcovskou konzoli. Všechny aktualizace musí být prováděny z webového prostředí bez potřeby asistence dodavatele/výrobce dodávaného systému. Požadujeme předložení posledních 4 poznámek k novému vydání (release notes) pro kontrolu parametrů navrhovaného systému.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/software/
3. Systém musí podporovat downgrade v jednom kroku, pro případ problémů s novou verzí systému po upgrade. Není přípustný downgrade pouze za součinnosti výrobce.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/logmanager-software-downgrade/
4. Průměrný trvalý příjem min. 10000 událostí/s. Výkon musí být dosažen na požadované množství událostí s průměrnou délkou zpráv minimálně 700Byte trvale. Systém musí prokazatelně kompletně zpracovat přijaté události včetně vytváření očekávaných metadat (DNS-PTR, čísla a jména ASN, geolokace), zajišťovat normalizaci, zamezovat ztrátě přijatých událostí nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu každé události.	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v datasheetu. Na následujícím odkazu je ke stažení Logmanager datasheet. https://logmanager.com/cs/podpora#documents-for-download
5. Špičkový příjem minimálně 20000 událostí/s po dobu nejméně 10 minut a průměrnou délkou minimálně 700byte. Systém musí prokazatelně kompletně zpracovat přijaté události, zamezovat ztrátě ukládaných dat nebo posunutí důvěryhodného časového razítka oproti času skutečného příjmu zpráv. Při zpracování dat během špičkového příjmu akceptujeme zpoždění zobrazení zpracovávaných dat. Systém ani ve špičkovém výkonu nesmí dovolit ztrátu dat, skluz důvěryhodného časového razítka nebo jiné prokazatelné vady na zpracovávaných datech oproti zpracování při průměrném trvalému příjmu událostí.	Zařízení splňuje požadavek. Viz tabulka „Technická specifikace“ v datasheetu. Na následujícím odkazu je ke stažení Logmanager datasheet. https://logmanager.com/cs/podpora#documents-for-download
6. Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den nebo licence na minimálně 500GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 120 TB a nad to musí podporovat kompresi ukládaných dat.	Zařízení splňuje požadavek. Na následujícím odkazu je ke stažení Logmanager datasheet. https://logmanager.com/cs/podpora#documents-for-download

Požadovaný parametr	Nabízená hodnota ¹
7. Uživatelská konfigurace klasifikace dat, parserů, filtrů a alertů se provádí pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát konfigurace bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou schémat-symbolů, které reprezentují aplikační logiku a kontrolují syntaxi. Doložte odkazem na dokumentaci systém vizuálního programování a popisu jednotlivých použitých komponent vizuálního programování nástroje.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/parsing-rules/ https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/
8. Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, čísel a jmen autonomních sítí, geolokační informace a identifikace výrobce zařízení podle MAC adresy.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/ https://doc.logmanager.com/latest/cz/suggestions-and-tech-tips/how-to-create-a-parsing-rule/ https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents/
9. Systém musí podporovat doplňování zpráv o informace z textových prohledávacích tabulek. (Například k uživatelskému jménu doplnit z textové prohledávací tabulky informaci o jeho emailu, členství v AD skupinách a podobně). Pro automatickou aktualizaci takto uložených doplňujících informací musejí být tyto textové prohledávací tabulky naplnitelné pomocí REST API nabízeného systému a modifikovatelné přes jednotné webové rozhraní.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/network/dns/
10. Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit skupinu testovacích zpráv, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení s upozorněním na chybná místa vytvářeného parseru. Pro snadnější vytváření parserů požadujeme mít možnost vložení minimálně 20 testovacích zpráv současně.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/classifiers/
11. V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. Systém obsahuje předdefinované značky, které automaticky přidává k přijímaným zprávám. Příklady značek: konfigurační změna, úspěšné ověření uživatele, neúspěšné ověření uživatele, zpráva přišla z windows, zpráva byla vygenerována firewallem atd.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/tags/

Požadovaný parametr	Nabízená hodnota ¹
12. Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/parser/ https://doc.logmanager.com/latest/cz/web-interface/parser/tags/
13. Pro možnost nasazení ve vysoké dostupnosti a výkonnostní rozšíření je vyžadována podpora sestavení ve vysoké dostupnosti – požadujeme podporu minimálně 4 nodů v clusteru. Nastavení clusteru se musí kompletně realizovat v grafickém rozhraní správcovské konzole v jednom kroku, není přípustné konfigurovat sestavení scripty, makry nebo úpravou textové konfigurace systému a pomocí ručních restartů služeb. Systém ve vysoké dostupnosti musí přehledně informovat o stavu clusteru a procesu synchronizace databází. Dokumentace k realizaci vysoké dostupnosti musí být kompletní a popisovat všechny kroky sestavování a obnovení v případě výpadku komponenty clusteru.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/cluster/ https://doc.logmanager.com/latest/cz/web-interface/system/task-status/ https://doc.logmanager.com/latest/cz/web-interface/system/software/
14. Vícenodový cluster se chová i ovládá jako jednotný systém, nutnost nezávislé konfigurace na každé jednotce v clusteru je vyloučena. Vícenodový cluster umožňuje geolokační oddělení a pro komunikaci v rámci clusteru musí využívat definovaný TCP/UDP port pro snadné nastavení prostupy firewallu. Veškerá komunikace v rámci clusteru musí být šifrovaná s vysokým kryptografickým standardem pro bezpečné vytvoření privátní virtuální sítě na síťové vrstvě.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/cluster/ https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager/
15. V případě rozšíření systému na cluster musí navrhovaný systém zajistit bezvýpadkovost sběru logů.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/cluster/
16. Systém musí umožňovat export dat ve formátu vhodném pro další strojové zpracování bez dodatečných omezení na časové období, množství nebo obsah exportovaných dat. Během exportu je možné označit pouze vybraná pole, která mají být do exportu zahrnuta.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/reports/
17. Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. Doložte odkazem na dokumentaci, jakým způsobem se provádí zálohování a obnova konfigurace systému.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/
18. Podpora důvěryhodného zálohování dat na externí systém. Požadováno plánované i ad-hoc zálohování. Zálohy dat musejí být vhodně kompresovány a umožnit v budoucnosti obnovení bez ohledu na verzi systému, ve které byla záloha pořízena.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/system/backup-restore/

Požadovaný parametr	Nabízená hodnota ¹
19. Systém je schopen na základě uživatelsky zadaných podmínek splněných v přijatých datech vygenerovat alert.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/templates/
20. Text emailu vygenerovaného alertem musí být uživatelsky definovatelný s proměnnými, které jsou vyplněny z přijaté rozparsované události.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/templates/
21. Systém musí obsahovat výrobcem předpřipravené sety/vzory alertů a korelací.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/alerts/ https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/
22. Systém musí provádět konfigurace alertů a korelací pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován čistě textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu. Konfigurace alertů musí umožňovat okamžitou kontrolu funkčnosti výstupu alertu nebo korelace vložení příslušné testovací zprávy, včetně zobrazení upozornění na případné uživatelské chyby.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/alerts/ https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/
23. Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala, na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. U Syslog protokolu požadujeme možnost definice formátu odesílaných dat pro snazší integraci se systémy třetích stran.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/alerts/ https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/
24. V alertech je možné nejen využívat, ale i přiřazovat značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru a je označen názvem lokality, nebo pokud událost obsahuje podmínku, přiřaď novou značku).	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/additional-informations/events-processing-in-blockly/defined-xml-blocks/special-blocks/special-elements/send-alert/ https://doc.logmanager.com/latest/cz/web-interface/logs/alerts/
25. Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. Definice korelačních pravidel je prováděna pomocí vizuálního programovacího jazyka a musí obsahovat možnost vložení testovací zprávy a zobrazení výsledku testu o provedené akci.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/logs/alerts/ dále Logmanager datasheet: https://logmanager.com/cs/podpora#documents-for-download

Požadovaný parametr	Nabízená hodnota ¹
26. 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 textových souborových logů. Agent se nesmí instalovat individuálně, ale prostřednictvím MS AD Group Policy a nesmí vyžadovat žádnou konfiguraci na cílovém systému.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-agents/
27. Filtrace odesílaných událostí agenty se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole systému. Logy nastavené k filtraci jsou filtrovány na straně windows agenta a nejsou nijak odesílány po síti. Vizuální programovací jazyk není prezentován textově, ale textově-grafickou formou, která vizualizuje aplikační logiku vytvářeného alertu.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-beats-agent/beats-global-config/
28. Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a jeho konfigurace musí být kompletně realizována v grafickém rozhraní systému bez využití skriptů nebo maker. Konfigurace musí být automaticky distribuována přímo z centrální konzole systému. Tj. vlastní správa a aktualizace Windows agenta se neprovádí z Group Policy.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/sources/windows/ https://doc.logmanager.com/latest/cz/web-interface/sources/windows-settings/
29. Komunikace Windows agenta a centrálního systému musí být zabezpečena TLS 1.2 a výše a musí podporovat ověřování certifikátem.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/sources/windows/
30. Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole v grafickém rozhraní nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. Dále musí Windows agent podporovat centralizované nastavení z administrátorské konzole systému pro sběr textových logů včetně možnosti výběru jejich formátu.	Zařízení splňuje požadavek Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/sources/windows/ https://doc.logmanager.com/latest/cz/logmanager-beats-agent/logmanager-orchestrator/
31. Windows agent musí automaticky doplňovat ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. K bezpečnostním událostem hodným pozornosti doplňuje značku a popis dle MITRE ATT&CK® matrice a k takto detekovaným procesům a souborům automaticky vytváří SHA256 hash.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/sources/windows-settings/ https://doc.logmanager.com/latest/cz/web-interface/sources/windows-filters/ https://doc.logmanager.com/latest/cz/web-interface/sources/windows/
32. Systém musí obsahovat centrálně spravované řešení, které umožňuje v budoucnu sbírat události na pobočkách a umožnit jejich odeslání po saturované lince bez ztráty dat.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-forwarder/logmanager-forwarder/

Požadovaný parametr	Nabízená hodnota ¹
33. Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat včetně dokumentace požadavků na virtualizaci a komunikační matici pro šifrovaný přenos dat.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/web-interface/
34. Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.	Zařízení splňuje požadavek. Viz dokumentace: https://doc.logmanager.com/latest/cz/logmanager-forwarder/logmanager-forwarder/
35. Řešení musí komunikovat po definovaném TCP/UDP portu, aby mohl být snadno nastaven přístup přes firewall a řešena kvalita služby (QoS) pro přenos událostí.	Komunikační matice Logmanageru: https://doc.logmanager.com/latest/cz/additional-informations/communication-of-logmanager/
36. Systém musí podporovat vygenerování TSR (technického support reportu) pro možnost diagnostiky bez vzdáleného přístupu.	Zařízení splňuje požadavek. TSR se vytváří se tak, že po přihlášení administrátora do Logmanageru se v URL prohlížeče nechá jen adresa Logmanageru a za ni se připojí tento řetězec /APIv1/system/config/support_info Logmanager zahájí vytváření tohoto TSR souboru (support_info.bin). Tento *.bin soubor pak uloží Logmanager Technické podpoře na jejich NextCloud web na unikátní adresu, kterou po otevření ticketu získá zákazník nebo partner od technika podpory Logmanageru. Technik Logmanageru pak má k dispozici vše, co je potřeba pro analýzu problému nebo diagnostiku systému bez nutnosti vzdáleného přístupu. *.bin soubor neobsahuje žádná zákaznická data (vyjma logu práce vlastního Logmanageru) a je šifrován.

Součástí dodávky je:

1. Dodávka do místa plnění.
2. Instalace, zapojení a základní konfigurace dodávaného logovacího systému dle požadavků Kupujícího v rozsahu maximálně 3 MD.
3. Projektové vedení, analytické práce, projektová, instalační a uživatelská dokumentace, integrace do havarijních plánů.

Popis Akceptačních testů

Číslo testu	Popis testu	Výsledek
1	Systém je nainstalován na určeném místě a je připojen k napájení.	Ano / Ne
2	Systém je redundantně připojen do sítě (LACP protokol) a jeho management je přístupný správcům. Otestováno odpojováním jednotlivých portů v LACP skupině.	Ano / Ne
3	Management konzole systému je dostupná pouze přes https rozhraní.	Ano / Ne
4	Do managementu systému je možné přihlásit.	Ano / Ne
5	Systém má nastaven NTP server pro synchronizaci času. Synchronizace byla ověřena.	Ano / Ne

Číslo testu	Popis testu	Výsledek
6	Systém má nastaven SMTP server a jeho parametry pro odesílání pošty, testovacím emailem byla otestována funkčnost nastavení.	Ano / Ne
7	Systém je spojen v cluster režimu a dnešní data a konfigurace je živě synchronizována.	Ano / Ne
8	Probíhá synchronizace starších indexů. Tato synchronizace bude probíhat vzhledem k velkému množství dat zhruba 1-2 měsíce.	Ano / Ne
9	Byla provedena rekonfigurace sítě a vytvořena IP adresa pro dosažení vysoké dostupnosti dle návodu výrobce na adrese https://doc.logmanager.com/latest/cz/additional-informations/logmanager-with-high-availability/	Ano / Ne
10	Byla otestována vysoká dostupnost logování pomocí odpojení/vypnutí primárního Logmanager serveru. Nadřazený Firewall začal automaticky směřovat data na zbývající funkční nody v clusteru. Slave node data přijímá, alertuje a ukládá do fronty. Viz popis v dokumentaci https://doc.logmanager.com/latest/cz/web-interface/system/cluster/#recovery-workflow-on-cluster-hw-failure--disaster-recovery	Ano / Ne
11	Po opětovném připojení master serveru došlo automaticky k opětovné synchronizaci uložených dat, konfigurace a ke zpracování fronty z doby výpadku.	Ano / Ne
12	Byla otestována vysoká dostupnost logování pomocí odpojení/vypnutí sekundárního Logmanager serveru. Nadřazený Firewall začal automaticky směřovat data na zbývající funkční nody v clusteru. Master node data přijímá, alertuje a ukládá do databáze.	Ano / Ne
13	Po opětovném připojení slave serveru došlo automaticky k opětovné synchronizaci uložených dat, konfigurace a ke zpracování fronty z doby výpadku.	Ano / Ne
14	Administrátoři objednatelů byli seznámeni a proškoleni k ovládání systému.	Ano / Ne

Seznam podporovaných systémů

Minimální seznam podporovaných zdrojů logů	k 19.3.2024
AIP Safe	
Apache httpd	
Apache Tomcat	
Amavis	
Antivir AVG	
Antivir Avast	
Antivir Eset Remote administrator	
Brocade FC switches	
ArcSight CEF (generický/standardizovaný formát)	
Barracuda Email Security Gateway	
Cisco ASA	
Cisco ASA-Lite (optimalizované pro výkon)	
Cisco Firepower	
Cisco ISE	

Minimální seznam podporovaných zdrojů logů	k 19.3.2024
Cisco IOS	
Cisco IronPort	
Cisco Nexus	
Cisco SMB	
Cisco UCS	
Cisco WLC	
CompuNet GAMA	
Dell Force10	
Dell iDrac (Server OoB management)	
Dell Isilon	
Dell PowerConnect	
Dell SonicWALL	
Dell W-series WiFi	
Discard (speciální pravidlo na fitrování událostí)	
Dropbear SSH (~součást Embedded Linux distribucí)	
Epacs (http://www.epacs.cz/)	
Extreme NAC	
Extreme Networks XOS	
FlowMon	
FortiAuthenticator	
FortiDDoS	
Fortigate	
FortiGate-Lite (optimalizované pro výkon)	
FortiMail	
FortiManager	
FortiADC	
FortiSandbox	
FortiWeb	
F5 BigIP ASM	
FreeRADIUS	
Greycortex NTA	
Qradar LEEF (generický/standardizovaný formát)	
H3C networking	
HAProxy (structured rfc5425 logformat)	
Hillstone NGFW	
HPE Aruba Instant AP (WLAN)	
HPE Aruba Clearpass	
HPE Aruba Mobility Controller (WLAN)	
HPE iLo (Server OoB management)	
HPE IMC	

Minimální seznam podporovaných zdrojů logů	k 19.3.2024
HPE routers	
HPE switches Aruba OS	
HPE switches Aruba-CX OS	
HPE switches Comware OS	
HPE Comware WLAN	
Huawei USG	
IceWarp	
CheckPoint LOG Exporter Lite (optimalizován na výkon)	
CheckPoint LOG Exporter	
ISC BIND	
ISC DHCP	
Jivex	
JSON (generický/standardizovaný formát)	
Juniper SRX	
Juniper SRX-Lite (optimalizované pro výkon)	
Kaspersky Endpoint Security	
Kaspersky Security Center	
Kemp LoadMaster	
Kerio Connect	
Kerio Control	
Kernun Clear Web	
Kernun Web filter	
Lenovo XClarity (Server OoB management)	
Linux Bash commands log	
Linux Cron	
Linux Freeradius	
Linux Iptables	
Linux Postfix	
Mikrotik	
Microsoft365 (API)	
Microsoft Exchange	
Microsoft Exchange tracking textový log (2010-2019)	
Microsoft SharePoint	
Microsoft SQL	
Microsoft Windows Defender	
Microsoft Windows DHCP textový log	
Microsoft Windows DNS debug textový log	
Microsoft Windows Firewall (EVTx i textový log)	
Microsoft Windows IIS / FTP server textový log	
Microsoft Windows IIS / Webserver textový log	

Minimální seznam podporovaných zdrojů logů	k 19.3.2024
Microsoft Windows logy z Event View (libovolný EVTx adresář)	
Microsoft Windows logy z libovolného textového souboru	
Microsoft Windows Sysmon	
MySQL	
Nginx	
Novell eDirectory	
Office365	
OpenSSH server	
Oracle DB	
Palo Alto Networks NGFW	
PostgreSQL	
Pulse Secure	
Qnap	
Ruckuss wireless	
Safetica DLP	
SAP (SM19 a SM20 logy)	
Shorewall	
Siemens Scalance	
SonicWall	
Sophos	
SpamAssasin	
Stapro FONS Enterprise, Akord, Openlims	
Squid (Web Proxy)	
Squid for Windows	
Radware Defense Pro	
RFC5425 (generický/standardizovaný formát)	
Symantec Endpoint Protection Manager	
Symantec Messaging Gateway (Brightmail)	
Synology NAS DSM	
Trapeze	
Trend Micro Apex One	
TrendMicro DeepDiscovery	
TrendMicro DeepSecurity	
TrendMicro TippingPoint	
TrendMicro Vision One	
UBNT Rocket	
UBNT UniFI	
Vectra Contigo	
VEEAM Backup and Restore	
Vmware vCenter a ESXi (až do verze 8.0.2 přes API)	

Minimální seznam podporovaných zdrojů logů	k 19.3.2024
Vmware Horizon	
Whalebone.io (DNS server)	
Zimbra	
Zyxel	

Vzorový návod – napojení Zabbix



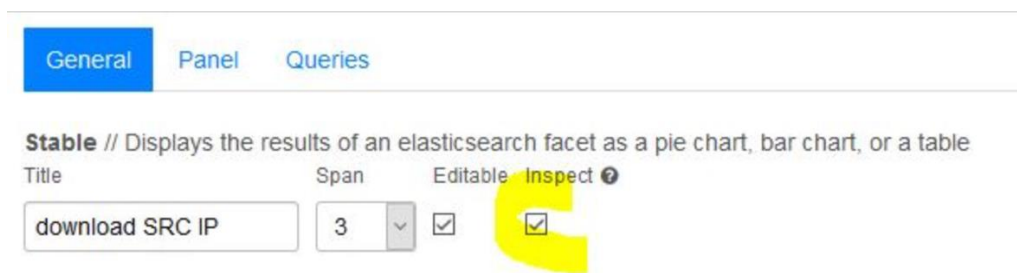
Logmanager – Napojení na monitorovací nástroj Zabbix pomocí REST API

23.7.2024

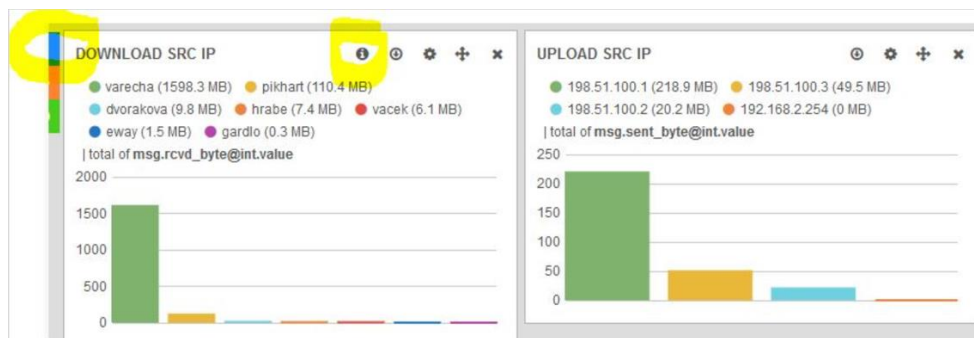
Tento návod bude přímo navazovat na příspěvek z fóra, kde bylo ukázáno, jak vyčítat pomocí REST API a BASH informace z kteréhokoliv grafu/tabulky v LOGmanageru. K napojení je využito Python skriptu, který bude vracet JSON formát pro Zabbix a následně pomocí JSONPath vyčítány jednotlivé hodnoty. Hodnoty, které jsou vyčítány v rámci návodu jsou stejné hodnoty, jako v případě vytvořeného dotazu na databázi z fóra.

1. Extrakce dotazu z Logmanageru

Nejprve je zapotřebí u chtěného grafu/tabulky zapnout inspekci, aby bylo možné vidět dotaz, který je bude dále používán k dotazování přes REST API.



Aby následně bylo možné vidět inspekci, je zapotřebí minimalizovat a maximalizovat řádek s grafem/tabulkou, poté bude možné na vrchní části grafu/tabulky písmenko „i“, pod kterým je vidět dotaz.



Poté je potřeba zkopírovat celý JSON dotaz, který začíná první „{“ a končí „}“ a to bez apostrofů u závorek. Tento zkopírovaný dotaz je poté potřeba upravit do řádku a to pomocí [odkazu](#), kam se vloží JSON dotaz a zmáčkne se „JSON Minify“.

Výsledná úprava JSON bude vypadat takto:

```
{
  "facets": {
    "terms": {
      "terms_stats": {
        "value_field": "msg.rcvd_byte@int.value",
        "key_field": "msg.username.raw",
        "size": 10,
        "order": "total",
        "facet_filter": {
          "fqquery": {
            "query": {
              "filter": {
                "query": {
                  "bool": {
                    "should": [
                      {
                        "query_string": {
                          "query": "msg.protocol:\\\"udp\\\" AND (msg.src_iface: ssl.* OR msg.dst_iface: ssl.* )",
                          "query_string": {
                            "query": "msg.protocol:\\\"tcp\\\" AND (msg.src_iface: ssl.* OR msg.dst_iface: ssl.* )",
                            "query_string": {
                              "query": "msg.protocol:\\\"icmp\\\" AND (msg.src_iface: ssl.* OR msg.dst_iface: ssl.* )"
                            }
                          }
                        }
                      }
                    ]
                  }
                }
              }
            }
          }
        }
      }
    }
  }
}
```

Tento dotaz bude dále upraven a použit k dotázání na Elasticsearch pomocí REST API.

2. Napojení na Zabbix pomocí REST API a python skriptu

Na napojení Zabbixu na REST API LOGmanageru je využito spouštění Python skriptu, který je nahrán do složky „ExternalScripts“ a pomocí UserParameter je spouštěn a vyčítány hodnoty.

Nejprve je potřeba zjistit, kde se nachází složka pro spouštění externích skriptů. V mém případě /usr/lib/zabbix/externalscripts.

```
root@zabbix: /usr/lib/zabbix/externalscripts# cat /etc/zabbix/zabbix_server.conf | grep "ExternalScripts"
### Option: ExternalScripts
# ExternalScripts=${datadir}/zabbix/externalscripts
ExternalScripts=/usr/lib/zabbix/externalscripts
```

Poté je potřeba vytvořit v této složce Python skript např. my_script.py, změnit práva, vlastníka a skupinu na skriptu.

Změna práv na skriptu:

```
sudo chmod 755 my_script.py
```

Změna vlastníka a skupiny na skriptu:

```
sudo chown zabbix:zabbix my_script.py
```

Dále je potřeba nastavit UserParameter v konfiguraci Zabbix agenta, který obsahuje klíč a command na spuštění skriptu. Pro konfiguraci agenta je potřeba editovat soubor /etc/zabbix/zabbix_agentd.conf. V konfiguračním souboru nelézt nastavení parametru a nastavit v pořadí <key>,<command>.

```
UserParameter=my_script,python3 /usr/lib/zabbix/externalscripts/my_script.py
```

Nastavení vypadá takto:

```
### Option: UserParameter
#   User-defined parameter to monitor. There can be several user-defined parameters.
#   Format: UserParameter=<key>,<shell command>
#   See 'zabbix_agentd' directory for examples.
#
# Mandatory: no
# Default:
UserParameter=my_script,python3 /usr/lib/zabbix/externalscripts/my_script.py
```

Po nastavení parametru je zapotřebí restartovat agenta.

```
sudo service zabbix-agent restart
```

Nyní je potřeba nastavit Python skript, kde je nutné upravit některé hodnoty a zkopírovat do skriptu upravený JSON. Červeně zvýrazněné hodnoty je možné upravovat a nastavovat na vámi zadané hodnoty.

V případě proměnné `datum_yesterday` je možné nastavit kolik indexů databáze se zpětně bude prohledávat (v mém případě poslední 2 dny), pomocí zvýrazněné hodnoty lze měnit.

Proměnná `epoch_start_change` je nastavena na dotazování se 24h zpět, lze změnit „hours“ za „minutes“, případně „days“.

Dále je potřeba nastavit IP adresu/DNS název pro LOGmanager (`LOGmanager_IP`) a uživatelské jméno/heslo (`username`, `password`).

Upravený JSON je potřeba zkopírovat do proměnné `query` a to mezi trojici uvozovek ("""). Potřebné je také změnit `@timestamp` hodnotu, a to ve formátu `"from": """+epoch_start1+""", "to": """+epoch_now+"""`. V poslední řadě je pak důležité ke všem zpětným lomítkům přidat ještě jedno, aby nedošlo k jejich odstranění při spuštění skriptu.

Skript pro autentizaci a dotázání Elasticsearch DB s výstupem v JSON formátu:

```
import requests
import json
import urllib3
import datetime
import time

from requests import Response

urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)

# Time settings

datum_now=time.strftime("%Y.%m.%d")
datum_yesterday=datetime.date.fromordinal(datetime.date.today().toordinal()-
1).strftime("%Y.%m.%d")
epoch_now=str(int(round(time.time() * 1000)))

current_time = datetime.datetime.now()
epoch_start_change=current_time - datetime.timedelta(hours=24)
epoch_start1=str(int(epoch_start_change.timestamp() * 1000))

# Authentication

url = "https://LOGmanager_IP/APIv1/system/login"
payload = {"user":"username","pswd":"password"}
session = requests.session()
response = session.post(url,params=payload, verify=False, timeout=2)

urlget="https://LOGmanager_IP/lma-admin-"+datum_now+",lma-admin-"+datum_yester-
day+"/_search?pretty"

# Query

query="""{"facets":{"terms":{"terms_stats":{"value_field":"msg.rcvd_byte@int.va-
lue","key_field":"msg.username.raw","size":10,"order":"total"},"facet_fil-
ter":{"fquery":{"query":{"filte-
red":{"query":{"bool":{"should":[{"query_string":{"query":"msg.protocol:\\\"udp\\\"
AND (msg.src_iface: ssl.* OR msg.dst_iface: ssl.*
)}}}, {"query_string":{"query":"msg.protocol:\\\"tcp\\\" AND (msg.src_iface: ssl.*
OR msg.dst_iface: ssl.* )"}}, {"query_string":{"query":"msg.protocol:\\\"icmp\\\"
AND (msg.src_iface: ssl.* OR msg.dst_iface: ssl.* )}}}}},"fil-
ter":{"bool":{"must":[{"range":{"@timestamp":{"from": ""+epoch_start1+""},"to":
""+epoch_now+""}}}, {"fquery":{"query":{"query_string":{"query":"meta.tags:(\\\"f
ortigate\\\"")}}}, {"_ca-
che":true}}, {"fquery":{"query":{"query_string":{"query":"msg.type:(\\\"traffic\\\"
)}}}, {"_cache":true}}}}}}}}}},"size":0}"""

response = session.post(urlget,data=query)
print(response.text)
```

Po nastavení všech výše uvedených parametrů je zapotřebí v Zabbixu vytvořit „item“ (*Configuration -> Hosts -> Items -> Create item*) ve které se nastaví Name, Type (Zabbix agent), Key (nastavit stejný jako v konfiguraci Zabbix agenta), Type of information (nastavit na Text), Update interval a případně vytvořit nový název pro aplikaci.

Item Preprocessing

Name

Type

Key

Type of information

Update interval

History storage period

New application

Applications

Populates host inventory field

Description

Enabled ☒

Tímto se na serveru, kde je agent spustí skript, který vrácí JSON výstup na zadaný dotaz. Výstup lze nalézt v *Monitoring* -> *Latest data* -> *Hosts* (v mém případě zabbix server) -> *název itemu* -> *History*.

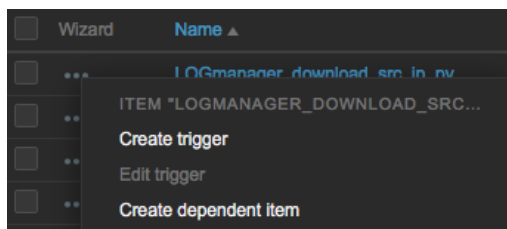
```

Timestamp      Value
2018-07-26 17:54:30 {
  "took" : 67,
  "timed_out" : false,
  "_shards" : {
    "total" : 6,
    "successful" : 6,
    "failed" : 0
  },
  "hits" : {
    "total" : 10397534,
    "max_score" : 0.0,
    "hits" : [ ]
  },
  "facets" : {
    "terms" : {
      "_type" : "terms_stats",
      "missing" : 0,
      "terms" : [ {
        "term" : "slechta",
        "count" : 12097,
        "total_count" : 11926,
        "min" : 0.0,
        "max" : 5.7908886E7,
        "total" : 3.047677155E9,
        "mean" : 255548.98163676003
      }, {
        "term" : "varechova",
        "count" : 799,
        "total_count" : 732,
        "min" : 70.0,
        "max" : 19787.0,
        "total" : 140353.0,
        "mean" : 191.73907103825135
      }, {
        "term" : "semionov",
        "count" : 1,
        "total_count" : 1,
        "min" : 3955.0,
        "max" : 3955.0,
        "total" : 3955.0,
        "mean" : 3955.0
      } ]
    }
  }
}

```



Nyní, když jsou výstupy z LOGmanageru nahrány v „itemu“ na Zabbix serveru, je potřeba vytvořit „Dependent item“ k výše uvedenému itemu.



Při vytváření závislé položky je potřeba, aby „Type“ byl nastaven na „Dependent item“, dále název nastaven na položku, na kterou se budeme dotazovat. Na příkladu níže je ukázáno, jak se budeme dotazovat na položku „total“, která uchovává celkovou velikost přenesených dat. Pro prvního uživatele je nastaven název na user[0].total, což odpovídá uživateli, který přenesl nejvíce dat. Nastaven „Key“ na název položky, kterou chceme monitorovat a „Type of information“ nastaven na „float“ z důvodu, že hodnoty nebudou celá čísla. V poslední řadě nastaven „Units“ na „B“, protože přijímaná hodnota je v bajtech.

Name: LOGmanager_download_src_ip_py: user[0].total

Type: Dependent item

Key: testlogpy.total

Master item: LOGmanager_download_src_ip_py: my_script

Type of information: Numeric (float)

Units: B

History storage period: 90d

Trend storage period: 365d

Show value: As is

New application:

Applications: -None-, CPU, Filesystems, General, Memory, Network interfaces, OS, Performance, počet jader

Populates host inventory field: -None-

Description:

Enabled: ☒

Buttons: Update, Clone, Clear history and trends, Delete, Cancel

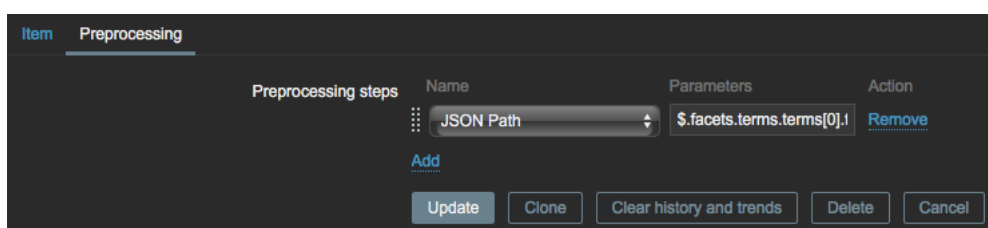


Po nastavení „itemu“ je potřeba nastavit na záložce „Preprocessing“ nastavit tzv. JSONPath, která je využita k získání konkrétní položky z JSON výstupu. Zde stačí nahrát JSON výstup, který je uložen v hlavním „itemu“ a vyzkoušet syntaxe k získání jednotlivých položek.

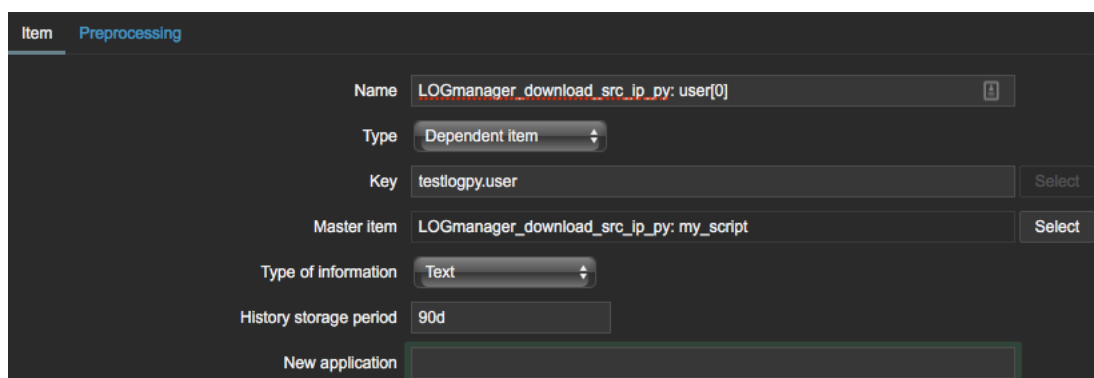
K získání „total“ je využita cesta:

```
$.facets.terms.terms[0].total
```

V „Preprocessing“ je potřeba zvolit JSON Path a vložit výše uvedenou cestu do „Parameters“.



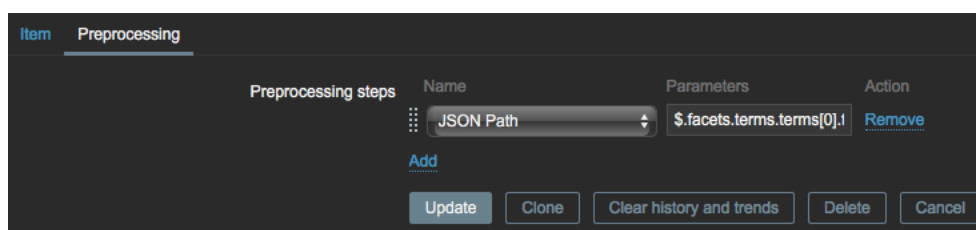
Stejným způsobem lze získat uživatelské jméno, kde je změněn pouze „Name“, „Key“ a „Type of information“ na text.



K získání uživatele „term“ je využita cesta:

```
$.facets.terms.terms[0].term
```

V „Preprocessing“ opět zvolit JSON Path vložit cestu.





Tímto způsobem lze získat všechny položky, které jsou v JSON výstupu obsaženy. V mém případě jsou získávání pouze uživatelé a velikost přenesených dat.

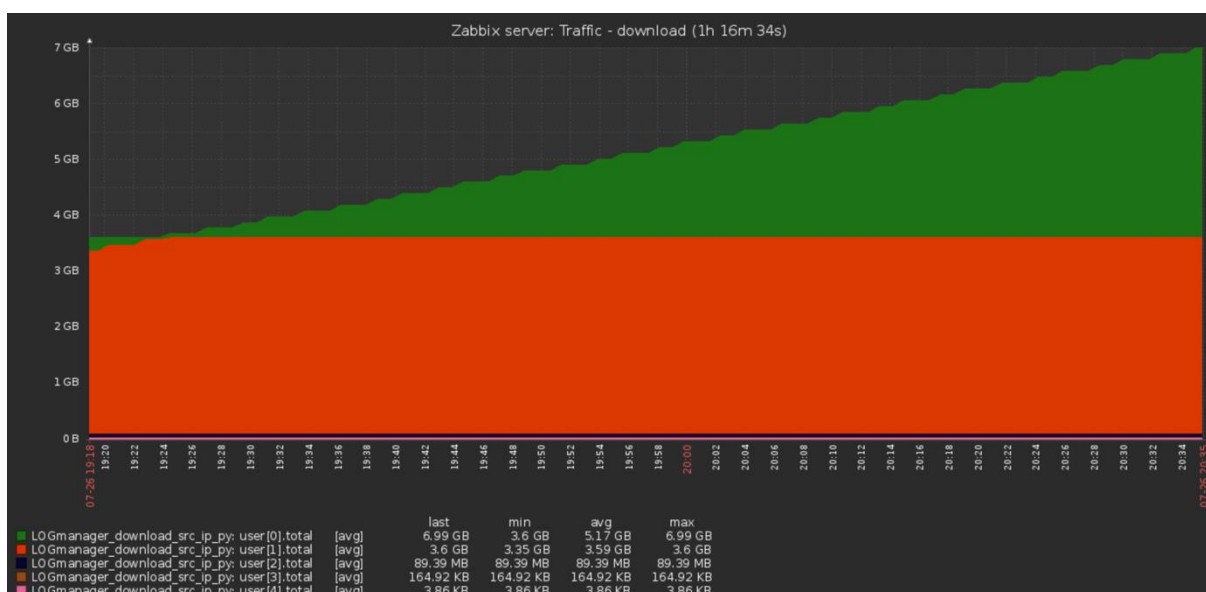
Wizard	Name ▲	Triggers	Key	Interval	History	Trends	Type	Applications	Status
☐	LOGmanager_download_src_ip_py		my_script	50s	90d		Zabbix agent (active)	python_api	Enabled
☐	LOGmanager_download_src_ip_py: LOGmanager_download_src_ip_py: user[0]		testlogpy.user	90d			Dependent item	python_api	Enabled
☐	LOGmanager_download_src_ip_py: LOGmanager_download_src_ip_py: user[0].total		testlogpy.total	90d	365d		Dependent item	python_api	Enabled
☐	LOGmanager_download_src_ip_py: LOGmanager_download_src_ip_py: user[1]		testlogpy.user1	90d			Dependent item	python_api	Enabled
☐	LOGmanager_download_src_ip_py: LOGmanager_download_src_ip_py: user[1].total		testlogpy.total1	90d	365d		Dependent item	python_api	Enabled

Pokud se podíváme do *Monitoring -> Latest data* je v první řadě vidět hlavní „item“, kde je celý JSON výstup a pod ním jednotlivé „Dependent itemy“ a jejich hodnoty. Díky tomu, že bylo nastaveno u hodnoty „total“ že je jedná o bajty, tak Zabbix automaticky převedl hodnoty (např. 3.864618915E9 na 3.6 GB).

python_api (11 items)			
☐	LOGmanager_download_src_ip_py	2018-07-26 20:34:19	{ "look": 105, "timed_out": ... } History
☐	LOGmanager_download_src_ip_py: user[0]	2018-07-26 20:34:19	pikhart History
☐	LOGmanager_download_src_ip_py: user[0].total	2018-07-26 20:34:19	6.89 GB +66.16 KB Graph
☐	LOGmanager_download_src_ip_py: user[1]	2018-07-26 20:34:19	slechtla History
☐	LOGmanager_download_src_ip_py: user[1].total	2018-07-26 20:34:19	3.6 GB Graph
☐	LOGmanager_download_src_ip_py: user[2]	2018-07-26 20:34:19	dvorakova History
☐	LOGmanager_download_src_ip_py: user[2].total	2018-07-26 20:34:19	89.39 MB Graph
☐	LOGmanager_download_src_ip_py: user[3]	2018-07-26 20:34:19	varechova History
☐	LOGmanager_download_src_ip_py: user[3].total	2018-07-26 20:34:19	164.92 KB Graph
☐	LOGmanager_download_src_ip_py: user[4]	2018-07-26 20:34:19	semonov History
☐	LOGmanager_download_src_ip_py: user[4].total	2018-07-26 20:34:19	3.86 KB Graph

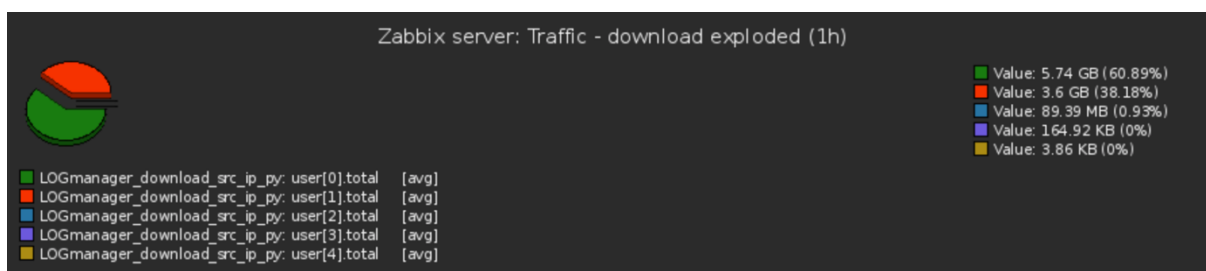
Z těchto hodnot lze vytvořit následně grafy, pro které jsou vybrány jednotlivé itemy (*Configuration -> Hosts -> Graphs -> Create graph*).

V mém případě standardní plošný graf:





Nebo třeba výšečový graf:



Jak už bylo poznamenáno, tímto způsobem lze vyčítat jakékoliv hodnoty z JSON výstupu a jednoduše nad nimi vytvořit grafy, případně „triggery“ na překročení hlídaných hodnot. Teď stačí už jen vytvořit v LOGmanageru dashboardy ze kterých budete chtít hlídat určité hodnoty a replikovat tento postup na ně.

O autorovi>

Kredit za tento dokument jde Matějovi Ryčkovi z Compunetu. Díky moc, Matěji.

./Míra