Příloha č. 2 – Seznam víceprací DCeGov

1 DCeGOV – fáze 3

1.1 Požadavek DCeGov (fáze 3)

1.1.1 Analýza

V rámci tohoto Změnového požadavku bude provedena analýza a návrh variant cílového řešení ukládání a zasílání auditních událostí aplikací IS eSeL.

Nově bude tato oblast realizována tak, že auditní události budou přímo zasílány do DCeGov.

Analýza bude obsahovat následující výstupy:

- návrh možných variant řešení
- stanovení výměnného formátu auditních záznamů (např. formát CEF)
- specifikace událostí, které budou do DCeGov předávány
- identifikace dopadů do infrastruktury eSeL
- identifikace dopadů do aplikačních částí eSeL
- způsob zabezpečení integrity auditních záznamů
- zabezpečení souladu výstupů s vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti
- stanovení pracnosti pro implementační fázi pro každou z variant

V rámci analýzy bude nutná součinnost NAKIT, a to v takovém rozsahu, aby vyjádření NAKIT (za projekt DCeGOV) bylo závazné. To bude znamenat zejména:

- odsouhlasení technických řešení jednotlivých variant
- předložení pracnosti řešení na straně DCeGOV ke každé variantě

Výstupem této analytické činnosti bude dokument, který bude obsahovat výše uvedená témata. Dokument bude využit pro následné rozhodnutí o technickém a procesním řešení.

Akceptace vícepráce DceGov bude v případě nedostupnosti bezpečnostního dohledu formou smoke testu.

1.1.2 Implementace

V rámci tohoto změnového požadavku bude implementována úprava logování aplikačních komponent takovým způsobem, aby vytvářené aplikační logy požadované VoKB umožňovaly jednoznačnou identifikaci záznamů určených pro předání do DCeGOV a zároveň umožňovaly oddělení těchto logů za účelem filtrování systémem Balabit tak, aby do DCeGOV mohly být předávány pouze pro něj určené logy.

Úprava logování bude spočívat ve vytvoření nového loggeru, který bude splňovat následující požadavky:

- Každý typ události, která bude vytvořena aplikací dle VoKB, bude mít jednoznačný identifikátor typu. Logger umožní konfiguračně (bez nutnosti úpravy aplikací) nastavit, zda daný typ událostí má nebo nemá být generován a následně předáván do DCeGOV a zda má být událost zaznamenána do auditního subsystému.
- Logger bude zaznamenávat své ID, na jehož základě bude možné logy dle VoKB identifikovat ve streamu logů z OCP. Události budou tedy zaznamenávány takovým způsobem, aby bylo možné je ve streamu logů z OCP identifikovat a následně oddělit a posílat prostřednictvím Balabit do samostatné destinace DCeGOV.

- Úpravy musí být kompatibilní se současným systémem logování v rámci EFK stacku a auditního subsystému.

Současně s implementací úprav budou v rámci tohoto změnového požadavku vytvořeny a předány vzory logů pro následující události zaznamenávané aplikačními komponentami systému:

- Přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů
- Činností provedených administrátory
- Úspěšné i neúspěšné manipulace s účty, oprávněními a právy
- Neprovedení činností v důsledku nedostatku přístupových práv a oprávnění
- Činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému (vztaženo převážně k administrátorům)
- Kritických i chybových hlášení technického aktiva
- Přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí

Vzory logů budou vytvořeny i pro relevantní podkategorie událostí.

Výstupem tohoto požadavku bude také první verze Katalogu logovaných událostí, který bude obsahovat:

- Typ události a její identifikátor
- Typ logu, tj. zda se jedná o událost zapisovanou do logu předávaného do DCeGOV, do auditní komponenty nebo do obou současně
- Identifikaci místa logování minimálně na úrovni aplikační komponenty a služby nebo funkce, která událost zaznamenává

1.2 Zdůvodnění

1.2.1 Analýza dopadů změn při předávání auditních událostí aplikací

V původním zadání byl požadavek na ukládání auditních událostí do auditní databáze. V tomto případě má mít bezpečnostní dohled možnost přístupu k těmto záznamům.

Tento změnový požadavek je realizován na základě požadavku Objednatele na změnu uchování auditních událostí, které mají být nově odesílány do DCeGOV a dále změny formátu, ve kterém mají být auditní události odesílány (formát CEF).

1.2.2 Implementace změn předávání auditních událostí aplikací

Implementační fáze bude vycházet z provedené analýzy, a na které se shodne Dodavatel a Objednatel jako na variantě určené k implementaci. Úpravy logování na aplikační úrovni jsou současně nutným předpokladem pro navazující fáze, v jejichž rámci bude implementováno rozdělování logů prostřednictvím Balabit tak, aby bylo napojení na DCeGOV realizováno v podobě vhodné pro provoz.

2 DCeGov – fáze 4

2.1 Požadavek

Tento změnový požadavek navazuje na DCeGov – fázi 3 a v jeho rámci bude provedena změna architektury řešení SSB (Balabit) na next-gen kaskádové zapojení, kdy je klíčový přesun některých funkcí filtrování na komponenty syslog relay virtuálních serverů.

Migrace architektury Balabit na next-gen kaskádové zapojení zahrnuje následující činnosti:

- Pro kaskádové zapojení budou provedeny rekonfigurace jak appliance SSB Balabit tak syslog relay serverů.
- Rekonfiguracemi bude zajištěna možnost filtrace, dělení a přeposílání vysokého objemu logů na virtuálních syslog relay serverech.
- Změna cesty logů, která umožní filtraci, dělení a přeposílání logů do DCeGov bez zapojení SSB appliance.
- Vytvoření nových filtrů pro požadované dělení aplikačních logů.

V rámci realizace tohoto požadavku bude v součinnosti s NAKIT finalizováno logování událostí dle VoKB z aplikačních komponent a finalizována dokumentace aplikačního auditního logování v Katalogu logovaných událostí.

2.2 Zdůvodnění

V původním zadání implementační analýzy nebyl požadavek na filtrování a dělení datových toků předávaných aplikačních logů OCP (OpenShift Container Platform) z IS eSeL do bezpečnostního monitoringu DCeGov. Tato změna řeší tyto filtrace a dělení a připravuje řešení na možnost škálování za účelem předávání vysokého objemu logů pomocí virtuálních syslog relay serverů.

2.2.1 Obsah aplikačních logů

Aplikační logy OCP IS eSeL obsahují záznamy generované PTA (podpůrných technických aktiv) typu

- aplikační server, platforma, framework, knihovna poskytující v kontejneru OCP služby backend aplikacím, včetně služeb run-time (běhového prostředí),
- nebo backend aplikace „spuštěné“ v kontejneru OCP.

2.2.2 Požadavky na předávané logy

Poskytování záznamů událostí DCeGov musí dle projektu odsouhlaseného SoKB splňovat tyto požadavky:

- logy PTA nesmí být po cestě do DCeGov modifikovány,
- logy daného PTA musí být do DCeGov poslány odděleně, v samostatném datovém streamu (síťově na různých cílových TCP portech).

- V případě OCP tak projekt požaduje
  - před zasíláním záznamů událostí z platformy OCP do KSM (Krajská sběrná místa) rozdělit datový tok záznamů dle výše uvedených typů: aplikační, infrastrukturní a auditní (je zajištěno současným Balabitem),
  - a tok záznamů událostí typu „aplikační“ na straně napojovaného systému ještě rozdělit dle podpůrných technických aktiv, která logují skrze OCP.
- OCP umožňuje dělit a posílat logy do různých destinací (ipaddr/protokol/port/SIEM konektor) podle NAMESPACE a typu OCP logu (auditní, infrastrukturní, aplikační) viz výše, čímž splňuje podmínku dělení logů OCP dle jejich typu (je zajištěno současným Balabitem).
- OCP ale neumožňuje dělit a odesílat aplikační logy OCP do různých destinací podle kontejneru a TPA „běžícího“ v kontejneru (podu). Tím nesplňuje požadavek na dělení datového toku aplikačních logů OCP dle PTA provozovaných v kontejnerech.

- V současné době je realizováno pouze dělení logů OCP dle jejich typu (na infrastrukturní, auditní a aplikační logy). Dělení aplikačních logů OCP dle PTA provozovaných v kontejnerech provedeno nebylo, a to z důvodu, že současný log management systém SSB (appliance Balabit) není dimenzován na požadované filtrování a dělení datových toků.

Tato změna řeší tyto filtrace a dělení a umožní zasílání logů dle požadavků na předávané logy popsaných v kapitole 2.2.2

3 DCeGov – fáze 5

3.1 Požadavek

Tento změnový požadavek navazuje na DCeGov – fázi 4 a jeho předmětem je optimalizace škálování výkonu filtrování logů předávaných do DCeGov.

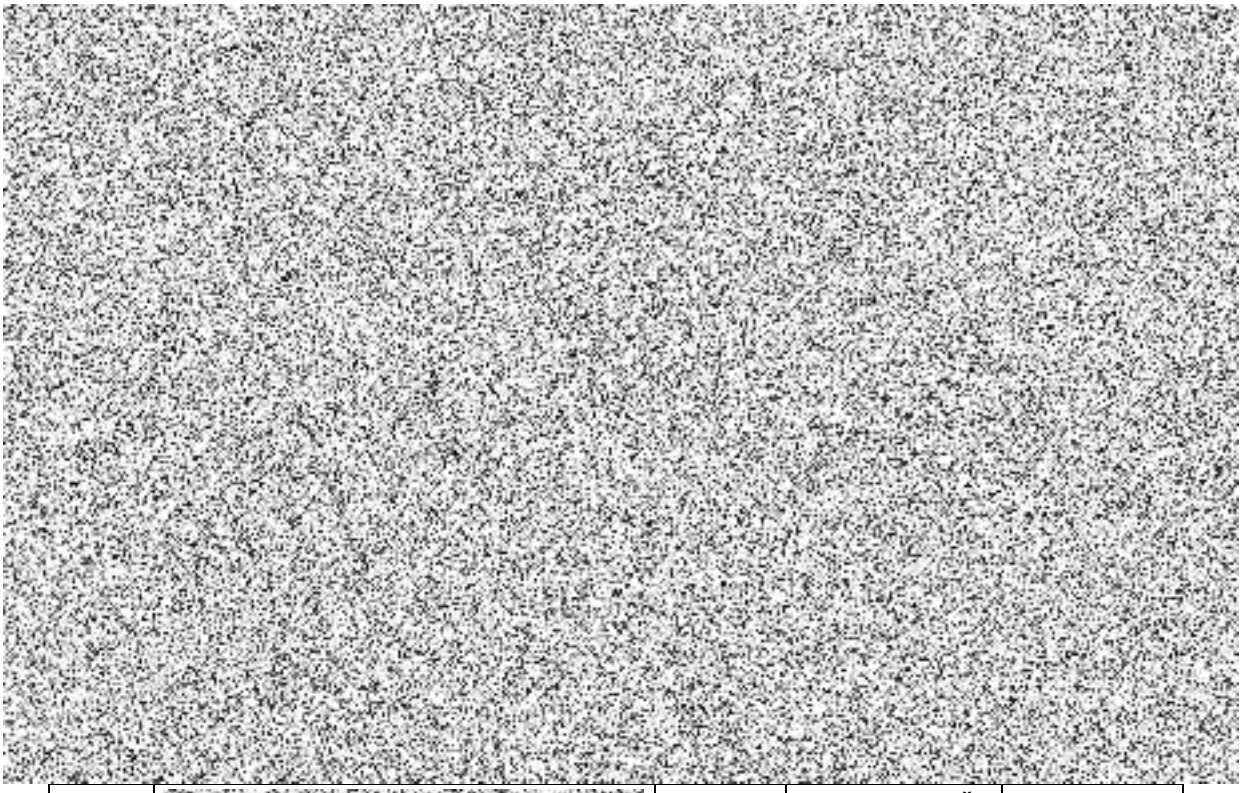
V rámci škálování výkonu filtrování budou realizovány následující činnosti:

- Dojde k otestování výkonu a škálování výkonu filtrování
- Dojde k optimalizaci výkonu a použitých zdrojů pro virtuální relay servery
- V případě potřeby pro zvýšení výkonu bude využito spuštění většího množství virtuálních syslog relay serverů v rámci volných zdrojů infrastruktury ESEL, úpravě konfigurace HA a Load Balancingu

3.2 Zdůvodnění

V původním zadání implementační analýzy nebyl požadavek na filtrování a dělení datových toků předávaných aplikačních logů OCP (OpenShift Container Platform) z IS eSeL do bezpečnostního monitoringu DCeGov. Současný log management systém SSB (appliance Balabit) není dimenzován na požadované filtrování a dělení datových toků. Tato změna řeší tyto filtrace a dělení a umožní škálování za účelem předávání vysokého objemu logů pomocí virtuálních syslog relay serverů.

4 Tabulka víceprací



			**2 531 808,00 Kč**	
	CELKEM včetně DPH po změnách		**3 063 487,68 Kč**