LogDock Advanced

Služba LogDock Advanced je cloudové řešení pro komplexní Log & Flow management. Služba poskytuje prostředí pro práci s událostmi a toky nejenom z IT infrastruktury zákazníka, ale i z jeho cloudových služeb. Umožňuje analyzovat a vyhodnocovat provozní a bezpečnostní incidenty.

Základem pro službu LogDock Advanced je softwarový nástroj pro sběr, ukládání, prohlížení a vyhodnocování provozních a bezpečnostních událostí a toků (logy). K nástroji má zákazník přístup přes webové rozhraní, ve kterém pracuje s uloženými logy. Logy mají 3 měsíční retenci, kterou lze na požádání navýšit.

- „Události" jsou záznamy ze síťových zařízení a aplikací. Služba podporuje protokoly událostí TCP/UDP Syslog. Pro sběr informací z Microsoft Windows poskytovatel doporučuje použít například WinCollect server. Po dohodě s poskytovatelem lze využít i jiné protokoly.
- „Toky" jsou záznamy o síťovém provozu, které generují obvykle síťová zařízení, jako jsou switche a routery. Podporované protokoly jsou Netflow, IPFIX, SFlow a JFlow.

Výkonnost služby je definována počty událostí za sekundu (Events per second – EPS) a toků za minutu (Flows per minute – FPM), které je služba schopna přijmout a zpracovat. Zákazník může objednávat tyto výkonnostní parametry:

- EPS VDC – definuje počet zpracovaných událostí z virtuálních firewallů a virtuálních load balancerů pouze v rámci služeb VDC Connect a VDC Connect Plus. EPS VDC lze škálovat po 20 ks.
- EPS – definuje počet zpracovaných událostí ze zákaznické cloudové i on-premise IT infrastruktury. EPS lze škálovat po 100 ks.
- FPM – definuje počet zpracovaných toků ze zákaznické on-premise IT infrastruktury. EPM lze škálovat po 5000 ks.

Výkonnostní parametry lze pružně měnit na měsíční bázi. V případě potřeby nabízí poskytovatel součinnost při odhadu počátečních hodnot.

Aby zákazník mohl využívat EPS a FPM, vytvoří mu poskytovatel za tímto účelem virtuální Event and Flow Processor (dále jen „Processor"). Processor umožňuje přijímat a zpracovávat události a toky ze zákaznické cloudové i on-premise IT infrastruktury.

Nutnou podmínkou pro zřízení služby LogDock Advanced je využívání služby VDC Connect nebo VDC Connect Plus.

Rozšíření a doplňkové služby

Zákazník si může ke službě doobjednat následující rozšíření:

- Report z logů ze služeb VDC Connect / VDC Connect Plus
- Report z logů ze služby VDC Connect Plus pro funkcionalitu Web Filterin.
- Reporty dle specifikace zákazníka
- Expertní podpora
- Instalace a školení v rozsahu 2MD

Reporty jsou zasílány dle volby zákazníka denně nebo jednou týdně (období sobota – pátek).

Ke službě lze dále zřídit následující doplňkovou službu:

- IPsec VPN – pro bezpečnou komunikaci z privátních sítí zákazníka

Doplňková služba je popsána v samostatném popisu služby IPsec VPN a je účtována zvlášť.

Komu je určena služba LogDock Advanced

Služba je určena pro všechny zákazníky vyžadující komplexní Log & Flow management z provozního, bezpečnostního či jiného pohledu.

Přínosy pro zákazníka

- jednotné místo pro správu provozních a bezpečnostních logů z celé infrastruktury
- založeno na jedné z nejlepších technologií na trhu
- odpadá starost o licence
- možnost neomezené doby ukládání Log & Flow
- zvýšení efektivity práce pomocí přehledných reportů
- napomáhá plnit soulad s požadavky zákona o kybernetické bezpečnosti
- Service Desk a lokální technická podpora v českém a anglickém jazyce 24/7

Odpovědnosti poskytovatele

- 8/5 správa a provoz platformy nezbytné pro běh služby
- 24/7 monitoring služby a dohled nad funkčností
- sběr logů ze služeb VDC Connect / VDC Connect Plus
- instalace, správa a provoz Processoru
- garantovaná dostupnost služby 95 % na schopnost přijímat a ukládat události a toky pro rozhraní Processoru
- garantovaná dostupnost webového rozhraní služby 95 %

Odpovědnosti zákazníka

- práce s prostředím, vytváření a správa náhledů na logy a další činnosti související s ovládáním služby přes webové rozhraní
- nastavení sběru Log & Flow na svých zařízeních (jiných než VDC Connect / VDC Connect Plus)
- plnit své povinnosti dle právních předpisů na ochranu osobních údajů a soukromí – zejména informovat dotčené subjekty o sběru a zpracování logů, získat jejich případný souhlas apod.

Parametry služby

Služba je účtována měsíčně dle následujících parametrů:

Účtovací jednotka	
EPS VDC	à 20 ks
EPS	à 100 ks
FPM	à 5000 ks
Processor (nutné pro EPS a FPM)	1 ks
reporty	1 ks
expertní podpora	à 15 min
instalace a školení	jednorázový poplatek
zvýšení retence EPS	à 100 EPS / 1 měsíc
zvýšení retence FPM	à 5000 FPM / 1 měsíc
snížení výkonnosti služby	jednorázový poplatek

Záruky poskytovatele

V případě nedostupnosti za každé 0,5 % nedostupnosti sleva 1 % z měsíčního paušálu (jednotlivě i kumulativně za všechny nedostupnosti nejvýše 100 %).

Důležité odkazy

Service Desk: https://www.serviceportal.dataspring.cz (doporučené prohlížeče jsou Firefox, Chrome a Safari), servicedesk@dataspring.cz, +420 222 74 40 13
eWiki: https://ewiki.dscen.cz/dokuwiki/doku.php