Podrobná specifikace Služeb datového centra (Technická specifikace řešení pro zajištění maximální dostupnosti mobilních a internetových aplikací OZP)

POPIS DOSAVADNÍHO (AKTUÁLNÍHO) STAVU PŘED ZAHÁJENÍM VEŘEJNÉ ZAKÁZKY

Stávající datové centrum Objednatele (dále též „OZP“) momentálně zajišťuje následující služby:

- Správu a pronájem prostředků pro provozování virtuálních serverů, na kterých běží servery webových a mobilních aplikací OZP (VMware)
- Správu a pronájem HW prostředků, nutných k oddělenému a bezpečnému provozování sítí použitých v mobilních a webových aplikacích OZP (Internet, DMZ, localnet, testnet).
- Oddělení bezpečnostních domén je řešeno minimálně na úrovni plně stavového firewallu.
- Správu a pronájem IT prostředků pro vytvoření VPN tunelů mezi datovým centrem, OZP a jednotlivými subUchazeči webových a mobilních aplikacích OZP přes Internetové připojení.
- Vlastní aplikace běží v produkčním prostředí a druhá oddělená infrastruktura je určena pro testovací a vývojové účely.

1 CÍLOVÝ STAV

Identické prostředí 1:1 vybudované tak, aby odpovídalo současnému prostředí.

- Redundantní řešení datového centra s kompletní replikací dat produkčního prostředí do druhé lokality.
- Redundantní spojení mezi OZP (budova Roškotova) a datovými centry prostřednictvím ISP připojení na obou stranách.

2 POŽADAVKY NA CÍLOVÉ ŘEŠENÍ REDUNDANTNÍHO DATOVÉHO CENTRA

Definice požadavku	Způsob splnění
Pro každé datové centrum dvě napájecí větve (různé fáze) s odolností vůči výpadku napájení (UPS, motor generátor) odpovídající TIER 3+.	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Vybavení každého datového centra automatickým hasicím systémem.	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Vybavení každého datového centra odpovídajícím systémem ventilace a klimatizace odpovídající TIER 3+.	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/ http://www.cloud4com.com/cloud4com/upload/File/c4c-technicka-specifikace-sluzeb.pdf
Pro každé datové centrum vytvoření a správa 3 bezpečnostních domén (Internet, DMZ a LOCAL), navzájem	Součástí řešení je Firewall FortiGate-VM00 Advanced Threat Protection (24x7 FortiCare plus Application

Příloha č. 1 Smlouvy o poskytování služeb datového centra

- **Podrobná specifikace Služeb datového centra**

Definice požadavku	Způsob splnění
oddělených minimálně plně dedikovanými stavovými firewally.	Control, IPS, AV and FortiSandbox Cloud) v režimu Active-Passive zahrnující správu v rozsahu 0.5 MD za měsíc.
Prostup mezi doménou Internet a LOCAL zabezpečený oddělením přes proxy server nebo firewall s plnou inspekcí na 7 vrstvě ISO OSI modelu.	Součástí řešení je Firewall FortiGate-VM00 Advanced Threat Protection (24x7 FortiCare plus Application Control, IPS, AV and FortiSandbox Cloud) v režimu Active-Passive zahrnující správu v rozsahu 0.5 MD za měsíc.
Nezávislé propojení bezpečnostních domén mezi datovými centry s následujícími parametry min. 10Gbit/s služby propojení datových center.	Propojení uvedených datových center je realizováno minimálně dvěma nezávislými 10Gbps spoji.
Minimálně 16 veřejně routovatelných a přenositelných IP adres (v.4) pro připojení do internetu dostupných v obou datových centrech + plná podpora pro IPv6 do Internetu.	Součástí nabídky je celkem 16 veřejně routovatelných a přenositelných IPv4 adres dostupných v obou uvedených datových centrech.
Přistup do Internetu realizovaný minimálně dvěma redundantními navzájem nezávislými přípojkami 10Gbit/s v každém DC.	Přístup do Internetu je realizovaný prostřednictvím tří nezávislých spojů v každém uvedeném datovém centru o kapacitě 10 Gbps.
Pronájem a správa HW a SW prostředků pro zajištění provozních a bezpečnostních požadavků webových a mobilních aplikací OZP.	Součástí nabídky je pronájem a plná správa požadovaných HW a SW prostředků.
Virtuální servery nesmí být připojeny přímo do Internetu.	Virtuální servery jsou připojeny do interních sítí dle požadavku zadavatele. Přístup do Internetu je realizovaný pomocí dedikovaného firewallu FortiGate
Přístup do internetu pro virtuální servery z DMZ domény musí být zajištěný minimálně plně stavovým firewallem.	Přístup do internetu pro virtuální servery z DMZ sítě/sítí je zajištěný pomocí dedikovaného plně stavového firewallu FortiGate
Přístup do Internetu pro virtuální servery z LOCAL musí být zcela oddělen prostřednictvím proxy serveru, případně firewallem s plnou inspekcí na 7 vrstvě ISO OSI modelu.	Přístup do internetu pro virtuální servery z LOCAL sítě/sítí je zcela oddělen pomocí dedikovaného plně stavového firewallu FortiGate s inspekcí na 7 vrstvě ISO OSI modelu.
Infrastruktura musí být schopna poskytnout tzv. SPAN port (zrcadlení veškerého definovaného provozu na fyzický port) pro monitoring a sledování bezpečnostních incidentů.	Nabízená infrastruktura podporuje tzv. SPAN port (zrcadlení veškerého definovaného provozu na fyzický port) pro monitoring a sledování bezpečnostních incidentů.
Automatický systém zálohování s minimální periodou pro zálohy 1 den pro primární i záložní datové centrum. Min 1x Full Backup/den Min 4x Incr/den doba obnovy dat RTO do 4 hodin doba uchování záloh min 1 měsíc uchování kopie záloh ve vzdálené lokalitě	Zálohování je řešeno pomocí SW Veeam Backup & Replication s plnou podporou požadovaných zálohovacích politik a uložení kopie záloh ve vzdálené lokalitě.
V případě výpadku primárního centra je záložní centrum schopno převzít produkční funkce webových a mobilních aplikací OZP do 4h (RTO max. = 4h) – požadavek pro DR. (redundantní infrastruktura bude postavena i v 2. DC)	Díky plné zastupitelnosti nabízené infrastruktury v záložním datovém centru je možné splnit požadavek na RTO max. = 4h pro DR. Všechny produkční virtuální servery jsou replikovány pomocí SW Veeam Backup & Replication.
Náběh záložního datového centra musí být konfigurován tak, aby nevyžadoval žádnou nebo minimální součinnost subjektů podílejících se na webových a mobilních aplikací OZP.	Náběh záložního datového centra je konfigurován s minimální požadovanou součinností subjektů podílejících se na aplikaci Vitakarta. Infrastruktura Primárního datového centra je provozována v HA režimu (HA cluster 2 ESXi hostů),

Příloha č. 1 Smlouvy o poskytování služeb datového centra

- **Podrobná specifikace Služeb datového centra**

Definice požadavku	Způsob splnění
Primární datové centrum musí být v HA režimu, odolné proti jakémukoliv výpadku jednotlivého HW prvku.	odolné proti jakémukoliv výpadku jednotlivého HW prvku.
HA řešení pro odolnost proti jakémukoliv jednotlivému výpadku není požadováno pro záložní datové centrum.	Z záložním datovém centru je provozován jeden ESXi host.
Záložní datové centrum nezávislé na hlavním datovém centru a to minimálně v rozsahu geografického oddělení z hlediska prostorů. Minimální vzdálenost nesmí být menší než 5 km.	Naše služby poskytujeme v následujících datových centrech, které splňují požadavky zadavatele: https://www.cra.cz/datove-centrum-dc-tower https://ttc-teleport.cz/datova-centra/
Aplikačně transparentní technologie pro šifrování dat v operačním systému s externím Key Management Serverem (KMS) s umístěním v lokalitě OZP.	Naše služba řešení s transparentním šifrováním dat v operačním systému s externím Key Management Serverem (KMS) s umístěním v lokalitě OZP podporuje díky technologii Thales (Gemalto) KeySecure a ProtectV. Služba není předmětem cenové kalkulace a je možné ji nacenit zvlášť dle požadavku zadavatele.
Připojení datových center s OZP a subUchazeči zajištěné prostřednictvím IPsec VPN se samostatnou větví pro provozní prostředí a samostatnou větví pro testovací a vývojové prostředí.	Součástí řešení je sestavení více IPsec Site2Site VPN pro bezpečný přístup do provozního a testovacího prostředí s ukončením VPN dle požadavku zákazníka.
Změny a provoz na testovacím či vývojovém prostředí nesmí ovlivnit provozní prostředí.	Prostředí jsou logicky oddělená a změny a provoz na testovacím či vývojovém prostředí neovlivní provozní prostředí.
Nedílnou součástí realizace je průběžná správa VPN připojení včetně přidání a modifikace VPN tunelů a sledování bezpečnostních incidentů.	Součástí řešení je průběžná správa VPN připojení včetně přidání a modifikace VPN tunelů a sledování bezpečnostních incidentů.
Pro každé datové centrum ve všech bezpečnostních doménách služba NTP časového normálu.	V každém datovém centru je dostupný NTP server.
Pro každé datové centrum ve všech bezpečnostních doménách služba SMTP relay pro odesílání mailů (pro domény LOCAL i přijímání mailů).	V každém datovém centru a všech bezpečnostních doménách je dostupný SMTP relay pro odesílání mailů (pro domény LOCAL i přijímání mailů).
Pro každé datové centrum ve všech bezpečnostních doménách služba DNS.	V každém datovém centru a všech bezpečnostních doménách je dostupná služba DNS.
Pro každé datové centrum ve všech bezpečnostních doménách přístup na definované služby v internetu – pro domény DMZ oddělení min. plně stavovým firewallem, pro domény LOCAL úplným oddělením (proxy), případně firewallem s plnou inspekcí paketů na 7 vrstvě ISO OSI modelu. Nedílnou součástí je správa firewallů	V každém datovém centru je dostupný spravovaný, dedikovaný a plně stavový firewall FortiGate-VM00 v režimu Active-Passive s inspekcí na 7 vrstvě ISO OSI modelu a oddělení bezpečnostních domén. Každá bezpečnostní doména má v každém datovém centru dedikovanou vlastní VLAN.
Pronájem místa v primárním datovém centru, včetně napájení a konektivity: 1x rack 1U server, 140W, připojení do lokální bezpečnostní domény, 2x PSU. Zajištění fyzického přístupu k zařízením spolu s poskytovatelem.	Součástí nabídky je požadovaný pronájem místa v primárním datovém centru, včetně napájení a konektivity: 1x rack 1U server, 140W, připojení do lokální bezpečnostní domény. Zajištění fyzického přístupu k zařízením je zajištěno spolu s poskytovatelem.
Pronájem místa v primárním datovém centru, včetně napájení a konektivity: 2x rack 2U server, 140W, připojení do lokální bezpečnostní domény, 2x PSU. Zajištění fyzického přístupu k zařízením spolu s poskytovatelem.	Součástí nabídky je požadovaný pronájem místa v primárním datovém centru, včetně napájení a konektivity: 2x rack 2U server, 140W, připojení do lokální bezpečnostní domény. Zajištění fyzického přístupu k zařízením je zajištěno spolu s poskytovatelem.

Příloha č. 1 Smlouvy o poskytování služeb datového centra

- **Podrobná specifikace Služeb datového centra**

Definice požadavku	Způsob splnění
Minimálně dalších 5U v datovém stojanu v primárním datovém centru.	Součástí nabídky je požadovaných 5U.

3 SEZNAM POŽADOVANÝCH VIRTUÁLNÍCH PROSTŘEDKŮ V DATOVÝCH CENTRECH

Položka	Položka technologická zkratka	Počet jader CPU	Velikost RAM (GB)	Velikost HDD (GB)	Rozhraní Ethernet 1 Gb
Provozní databázový server	VM-BVIT-DB-PROD	4	16	300	1
Testovací databázový server	VM-BVIT-DB	4	16	300	1
Provozní reverzní proxy server	VM-FE-PROXY-PROD	2	8	120	1
Testovací reverzní proxy server	VM-FE-PROXY	2	4	60	1
Poštovní server	VM-OZP-MAIL-PROD	2	2	20	1
Testovací www server	VM-OZP-WEB	2	4	62	1
Provozní www server statických stránek	VM-OZP-WEB-PROD	2	8	192	1
Provozní www server hlavních stránek	vm-atwebsite	4	12	160	1
Eshop	VM-VITASHOP-WEB	2	6	250	1
Flowmon kolektor	VM-FLOWMON	4	16	1091	4
AddNet workserver	VM-WORK-1	3	8	81	3
AddNet workserver	VM-WORK-2	3	8	81	3
Monet sonda	VM-MONET	3	8	81	1
Biztalk server produkční	VM-BTSEXT-PROD	4	16	650	1
Biztalk server školící	VM-BTSEXT-SK	4	8	350	1
Biztalk server testovací	VM-BTSEXT-TST	4	16	350	1
Aplikační server VITAKARTA	VM-BVIT-APP	4	8	150	1
poštovní server	VM-OZP-MAIL	2	2	20	1
Aplikační server VITAKARTA	VM-BVIT-APP-PROD	4	8	400	1
Aplikační server VITAKARTA eshop	VM-VITASHOP-WEB-PROD	10	16	400	1
Aplikační server VITAKARTA	VM-SCOMGW	2	4	60	1
Aplikační server VITAKARTA	VM-NS2	3	8	81	1
provozní server	vm-fp01	4	16	27	1
provozní server	vm-fp02	4	16	27	1
Kuberneter cluster	vm-vtk-k8s-master01	2	4	50	1
	vm-vtk-k8s-master02	2	4	50	1
	vm-vtk-k8s-master03	2	4	50	1
	vm-vtk-k8s-worker01	4	32	600	1
	vm-vtk-k8s-worker02	4	32	100	1
	vm-vtk-k8s-worker03	4	32	100	1
	vm-vtk-k8s-master01-test	2	4	50	1
	vm-vtk-k8s-worker01-test	4	8	100	1
NAS - na zálohy	zálohování prostředí	----------	----------	16000	1
Provozni: Vmware	ozp-dc1-vcenter	4	16	320	1

Provozni: Backup		ozp-dc1-vpr-0	4	6	40	1
Provozni: Network		ozp-dc1-fg	2	4	104	1
Provozni: Backup		ozp-dc2-vbck	2	6	80	1

4 KUBERNETES CLUSTER

Objednatel požaduje provést vytvoření a následný provoz 2 Kubernetes clusterů o následujících parametrech:

Definice požadavku	Způsob splnění
Instalace Kubernetes clusterů (K8s) verze 1.28 na virtuálních serverech dle specifikace v tabulce v odstavci 4	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
Produkční cluster o 6 virtuálních serverech: • 3 x control plane node • 3 x worker node	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
Testovací cluster o 2 virtuálních serverech: • 1 x control plane node • 1 x worker node	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
nastavení Linux distribuce Ubuntu 22.04 LTS pro provoz K8s	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
vysoce dostupné K8s API	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
K8s nginx ingress pro přístup k webovým aplikacím z vnějších sítí	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
vytvoření aplikačních namespaců dle potřeb vývojářů	Součástí nabídky je požadovaná služba Kubernetes clusteru s požadovanými parametry.
nastavení síťové bezpečnosti pomocí network policy, izolace v rámci namespace	Součástí nabídky je nastavení veškerých potřebných network policy s požadovanými parametry.
vytvoření personifikovaných přístupů pro vývojáře a nastavení oprávnění	Součástí nabídky je nastavení personifikovaných přístupů pro vývojáře a nastavení oprávnění
reporting K8s zátěžových metrik v reálném čase	Součástí nabídky je reporting K8s zátěžových metrik v reálném čase
nastavení priorit při alokaci zdrojů per aplikace	Součástí nabídky je nastavení priorit při alokaci zdrojů per aplikace
nastavení monitoringu virtuálních serverů	Součástí nabídky je nastavení monitoringu virtuálních serverů
nastavení monitoringu K8s clusteru	Součástí nabídky je nastavení monitoringu K8s clusteru
napojení clusteru na NFS úložišť	Součástí nabídky je napojení clusteru na NFS úložišť
otestování funkčnosti K8s clusterů • failover/failback jednotlivých komponent clusteru • hello world aplikace využívající komponenty K8s clusteru	Součástí nabídky je otestování funkčnosti K8s clusteru • failover/failback jednotlivých komponent clusteru • hello world aplikace využívající komponenty K8s clusteru
výstupem musí být plně funkční K8s clustery pro provoz aplikací	Součástí nabídky je plně funkční K8s cluster pro provoz aplikací
Provoz kuberenetes clusterů: • 24x7 dohled nad provozem K8s clusterů, řešení případných incidentů	Součástí nabídky je požadovaná služba Kubernetes clusteru s následujícími provozními parametry:

Definice požadavku	Způsob splnění
• aktualizace operačních systému virtuálních serverů, kvartálně • aktualizace K8s, ročně • kooperace s vývojáři při aktualizaci • zajištění odborné uživatelské a technické podpory (dostupnost přes helpdesk, email, telefon)	• 24x7 dohled nad provozem K8s clusteru, řešení případných incidentů • aktualizace operačních systému virtuálních serverů, kvartálně • aktualizace K8s, ročně • kooperace s vývojáři při aktualizaci • zajištění odborné uživatelské a technické podpory (dostupnost přes helpdesk, email, telefon)

5 Samoobslužný uživatelský portál pro řízení a správu zdrojů

Součást poskytovaných služeb „hostingu“ musí být uživatelský portál zpřístupněný Objednateli, v němž bude moct Objednatel na základě přístupových oprávnění administrátorsky provádět nejméně níže uvedené operace.

Definice základních vlastností portálu:

Název položky	Popis položky	Požadované funkcionality
Orchestrace serverové virtualizace	Služba poskytující škálovatelný samoobslužný přístup k výpočetním zdrojům.	Vytvoření instance
		Pozastavení instance
	Správa a automatizace velké množiny počítačových zdrojů.	Smazání instance
	Schopná pracovat s běžně dostupnými technologiemi virtualizace.	Zastavení instance
	Podpora hypervisorů: VMware – plně kompatibilní se současnou provozovanou platformou.	Změna velikosti instance
	Možnost horizontálního škálování na standardním hardwaru bez proprietárních požadavků na hardware či software.	Vytvoření snapshotu
		Přiřazení veřejné adresy
	Garance CPU Ready Time do 100ms pro každou provozovanou instanci včetně reportování parametrů.	Oddělení veřejné adresy
	Přístup k výkonnostním grafům a SLA reportům instancí.	Přiřazení skupiny firewall pravidel

Příloha č. 1 Smlouvy o poskytování služeb datového centra

- **Podrobná specifikace Služeb datového centra**

	Možnost instalace vlastního operačního systému instance z ISO obrazu.	Změna skupiny firewall pravidel
		Zobrazení výstupu konzole instance v prohlížeči
		Přidání/odebrání virtuálního síťového interface
		Spuštění instance
Orchestrace úložiště	Služba, která řídí vytváření, připojování a odpojování blokových zařízení k serverům.	Vytvoření volume
	Umí spolupracovat s různými druhy uložišt, jako jsou např.: CEPH, CloudByte, Coraid, EMC (ScaleIO, Vmax VNX a XtremIO), GlusterFS, Hitachi Data Systems, IBM Storage (IBM DS8000, Storwize family, SAN Volumee Controller, XIV Storage System a GPFS), Linux LIO, NetApp, Nexenta, Nimble Storage, Scality, SolidFire, HP (StoreVirtual a 3PAR StoreServ family) a Pure Storage.	Smazání volume
	Je vhodný pro výkonově náročné aplikace, jako je databázové úložiště, rozšiřitelné souborové systémy a poskytuje přístup serveru na úroveň bloku úložiště.	Přiřazení volume k instanci
	Poskytuje výkonné funkce pro zálohování dat uložených ve volumeech blokové storage.	Oddělení volume od instance
	Snapshoty mohou být obnoveny nebo použity k vytvoření nového volume.	Rozšíření volume
		Vytvoření volume z volume (klonování)
	Volumee	
	- logická jednotka, úložný prostor s jedním souborovým systémem, typicky leží na jednom oddílu pevného disku, velikostí se může lišit od fyzického disku	Migrace volume (asistovaná hostem)
	Přístup k výkonnostním grafům a reportům volumeů.	QoS – limity v IOPS

	Snapshoty	Vytvoření snapshotu volume
	- stav systému v určitém časovém okamžiku (na úložišti)	Smazání snapshotu volume
		Vylistování snapshotů
		Vytvoření volume ze snapshotu
Autentizace portálu	Identity služba zajišťující autentikaci skrze API klienta a autorizaci na vysoké úrovni.	Vytvoření role
		Smazání role
	Podporující 2-faktor autentizaci.	Vylistování rolí
		Vytvoření projektu/tenantu/vdc
		Smazání projektu/tenantu/vdc
	Role	Informace o projektu/tenantu/vdc
	-vytvoření a nastavení jednotlivých rolí podle jejich oprávnění	Vylistování projektů/tenantů/vdc
		Přiřazení uživatele do projektu/tenantu/vdc
	Tenant/Projekt	Odebrání uživatele z projektu/tenantu/vdc
	- skupina uživatelů používající omezené výpočetní zdroje	Vytvoření uživatelů
		Smazání uživatelů
		Vylistování uživatelů
		Nastavení hesla uživateli
		Přiřazení/odebrání rolí uživatelům
		Upravení informací o uživateli

Příloha č. 1 Smlouvy o poskytování služeb datového centra

- **Podrobná specifikace Služeb datového centra**

Orchestrace sítí	Služba doručující NaaS (networking as a service) ve virtualním výpočetním prostředí.	Vytvoření sítě
		Smazání sítě
	Možnost vytvořit bohaté síťové topologie a konfigurovat pokročilé síťové politiky v cloudu v hybridním prostředí sdílené a dedikované platformy.	Seznam sítí
		Informace o síti
	Možnost nasazení plně dedikovaného síťového řešení pro zajištění min. plně stavového firewallu, případně firewallu s plnou inspekcí paketů na 7 vrstvě ISO OSI modelu.	Vylistování všech sítí
		Informace o jednotlivých sítí a mapování do VLAN/VXLAN
		Vytvoření Poolu IP Adres
		Smazání Poolu IP Adres
		Seznam Poolu IP Adres
		Informace o Poolu IP Adres
	Security Groups (SG)	Vytvoření routeru
	- slouží jako virtuální firewall, který řídí průtok dat pro jednu nebo více instancí. Ke každé SG je možné přiřadit pravidla, které umožňují průtok dat do nebo z instancí.	Smazání routeru
		Nastavení brány routeru
		Odebrání brány routeru
		Seznam routerů
	Veřejný Pool IP	Informace o routeru
	- služba, která nepoužívá DHCP, k instancím s přiřazenou Pool IP lze přistupovat z veřejné sítě.	Přidání sítě do routeru
		Odebrání sítě z routeru
		Vytvoření SG firewallu
		Smazání SG firewallu

		Vylistování SG firewallu
		Vytvoření pravidla v SG firewallu
		Smazání pravidla v SG firewallu
		Vylistování pravidel v SG firewallu
		Informace o pravidlech v SG firewallu
API	REST API slouží pro programový, uživatelský a administrátorský přístup k poskytnutým zdrojům ve sdílené cloudové platformě.	K API musí být dostupná kompletní dokumentace.
		API komunikace výhradně přes SSL.
		API příkazy musí být autentikovány a ověřeny.
CMDB (Configuration management database)	CMDB je zde jako centrální úložiště všech konfigurací systému, tak aby se dali ukládat ve verzovacím nástroji pro sledování a audit změn. CMDB slouží jako vstupní bod pro aktualizace, záplaty, opravy, updaty a upgrady systému.	Kontinuální konfigurace a řízení změn pro zachování konzistence napříč všemi komponentami.
		Centrální místo pro zjišťování současného stavu konfigurací komponent.
		Efektivní a automatizovatelné nasazení produkčních částí systému.
		Centrální místo pro zjišťování stavu systémů (IP, OS, verze instalovaných aplikací, atp.)
Logování, monitoring a události		Nástroj má schopnost exportovat svoje události do nadřazených systémů.
		Nástroj sbírá centrálně logy a zobrazuje je skrze webové rozhraní.