Standardy pro monitoring informačního systému Všeobecné zdravotní pojišťovny ČR

Informační architektura VZP ČR

Obsah

Historie dokumentu

Verze	Datum	Autor	Popis
1.00	1.6.2014	VZP ČR	Vytvoření dokumentu

Standardy monitorování provozu informačního systému

Dohled provozu informačního systému je centralizovaný a je zajišťován dohledovým centrem s dvousměnným provozem v pracovních dnech od 6:00 do 22:00 hod. (v režimu 5x16). V těchto časových úsecích jsou drženy pohotovosti řešitelských skupin pro síťovou infrastrukturu, operační systémy Unix, operační systémy Windows, Oracle databáze, provoz aplikací, Exchange a pro dohledové nástroje.

1 Prostředí a podmínky monitoringu

1.1 Používané dohledové nástroje

Centrální systém dohledu provozu informačního systému je vybudován na platformě HP OpenView. Do dohledového centra HP OMU (centrální konzole nástroje HP Operations Manager for Unix) jsou soustřeďovány všechny důležité zprávy z ostatních monitorovacích nástrojů. HP OMU je propojen s nástrojem Service Manager.

Klíčové síťové prvky jsou sledovány pomocí HP NNM. Vybrané události jsou integrovány do konzole HP OMU. Kvalitativní parametry sítí jsou monitorovány pomocí nástrojů v CiscoWorks LMS. Nástroj je plně v gesci OSI a není integrován s HP OMU.

Všechny infrastrukturní komponenty Oracle jsou monitorovány pomocí agentů Oracle Enterprise Manager (OEM) / Oracle Grid Control. Nástroj je v gesci OSAD a je integrován do centrální konzole HP OMU.

Sledování provozu, parametrů a funkčnosti služeb všech serverů Windows je zajištěno produktem MS System Center Operations Manager (SCOM) s integrací do HP OMU. Nástroj spravuje OSOS.

Monitoring uživatelské dostupnosti (aplikační monitoring) aplikací je nasazován pomocí HP Business Service Management (HP BSM). Tento nástroj je integrován do centrální konzole HP OMU, a to obousměrně.

Bez-agentní způsob sledování lze uskutečnit pomocí HP Sitescope.

Dále je aplikační monitoring provozován pomocí podpůrných nástrojů, zpravidla custom skriptů na různých platformách - OS shell, perl, java, AutoIT apod. Tyto nástroje jsou dodány spolu s aplikací nebo byly vytvořeny v součinnosti s dodavatelem a provozním správcem aplikace.

1.2 Návrh monitoringu

Každá nově dodávaná aplikace nebo komponenta infrastruktury musí být monitorována, a to před nasazením do provozu. Návrh sledování dostupnosti, chybovosti a výkonnosti nových služeb, klíčových aplikačních a systémových procesů a infrastrukturních komponent musí být součástí projektových dokumentů (analýzy, technického designu, funkčního designu, implementační dokumentace) a zejména administrátorské a provozní dokumentace.

Návrh monitoringu vychází z doporučení dodavatele a je vypracován v součinnosti s VZP.

Pro zadání a zejména evidenci monitoringu, tj. soupis služeb a jejich vazeb, infrastrukturních prvků, sledovaných událostí a metrik, jsou připraveny tabulky, které jsou součástí „Tabulek pro předávání aplikací do provozu“. Úsek ICT

Řešení musí obsahovat volbu monitorovacího nástroje a soupis případného dalšího software potřebného k monitoringu (např. komponent HP OMU – agentů, SPI, resp. management packs pro SCOM, umístění sond a jejich cílové URL).

Popis řešení musí vycházet z popisu služeb a procesů aplikace. Ke každé službě je nutné uvést, jakým způsobem lze zjišťovat její stav (např. běžící proces, záznamy v logu, případně sonda), u procesů jak zjistit, zda zpracovává příslušná data, případně úspěšnost průběhu (např. monitorováním stavů front požadavků). Informace o stavech služeb, procesů a infrastruktury musejí být

kategorizované dle závažnosti a musejí být stanoveny příslušné metriky, v případě potřeby víceúrovňově.

Součástí zadání do monitoringu musí být komunikační matice a popis řešení generovaných událostí:

- priorita řešení a závažnost události
- popis řešení události, případně puštění opravné akce (restartování služby, komponenty, spuštění skriptu)

Pro centrální aplikace je nutné připravit jednak monitoring dostupnosti aplikací a současně zabezpečit sledování i jejich funkčnosti a výkonnosti.

Řešení monitoringu musí být navrženo tak, aby sledovaných událostí bylo co nejméně, a sledování bylo proaktivní, tj. sledované události musejí včas upozornit na mezní stavy systému (překročení definovaných prahových hodnot), aby bylo možné reagovat a zabránit výpadku služby. Zpracování musí umožňovat i sledování plnění kvalitativních parametrů dle zadání.

Pokud dodávanou komponentu (aplikaci, systém, prvek infrastruktury) ze závažných důvodů nebude možné monitorovat přímo standardizovanými nástroji VZP ČR, musí být vždy události generované z jiného nástroje přenášeny v reálném čase do HP OMU, aby byly informace o stavu informačního systému VZP centralizovány na jednom místě. Licence takto dodaných nástrojů budou pořízeny z rozpočtu dodávané aplikace/komponenty.

Pořízení nového monitorovacího nástroje nebo řešení dohledu musí být předem projednáno a schváleno vedoucím Oddělení centrálního dohledu.

1.3 Rozhraní pro monitoring

V případě „nativního“ prostředí HP OMU (HP-UX) jsou pro sledování procesů a stavů systému použiti agenti HP OMU doplnění o SPI (Smart-Plugins) a potřebné šablony (templates).

Pro komponenty, na jejichž monitoring je použit nástroj Oracle Enterprise Manager / Grid Control, je nezbytné dodat seznam všech instancí Oracle komponent potřebných k chodu aplikace.

V HA aplikacích je nutné popsat režim, v němž jsou redundantní komponenty konfigurovány (loadbalance/failover) a určit závažnosti výpadků komponent a souvislosti kombinací těchto výpadků.

V případě monitorování pomocí logů (systémových, aplikačních apod.) musí být log v podobě cleartext souboru operačního systému, a to v některém ze všeobecně používaných formátů (Syslog, Common / Combined Log Format,…), případně lze použít interní formát VZP. Formát souboru musí být zpracovatelný (filtrovatelný) šablonami HP OMU. Cesta k logu a jeho název musí být vždy statické, pokud log rotuje, tak je nutné zajistit neměnnost názvu aktuálního monitorovaného logového souboru. Logový soubor musí být lokální, tj. agent nemůže k logu přistupovat pomocí síťového protokolu např. na sdíleném prostředí. To ale nevylučuje vzdálené plnění logu.

Jako nepřípustný pro automatizovaný monitoring je log v podobě průběžné databázové tabulky.

Na platformě Windows musí být formát logu zpracovatelný nástrojem SCOM (např. formát Event log).

Všechna klíčová síťová zařízení, servery a síťové tiskárny musejí mít implementován protokol SNMP s možností hlášení událostí pomocí SNMP trapů a MIB kompatibilní s aktuální MIB v HP OV NNM. Všechna klíčová síťová zařízení musejí podporovat protokol RADIUS.

2 Standardy infrastrukturního monitoringu

2.1 Standard pro monitoring síťové infrastruktury

Monitoring datových sítí (LAN i WAN) je primárně prováděn pomocí HP OpenView Network Node Manageru. Jsou sledovány klíčové prvky sítí (směrovače, přepínače, WAN akcelerátory, GSS, Load balancery), v případě potřeby jsou sledovány i další důležité prvky, např. servery.

Pro zavedení síťového prvku do sledování je potřeba předat IP adresu síťového prvku a masku sítě, FQDN prvku z DNS a verzi běžícího SNMP protokolu. Dále je potřeba zadat rozsah sledování – která síťová rozhraní sledovat, klasifikovat závažnost příchozích SNMP trapů, zadat, které OID se mají aktivně sledovat a s jakými limity.

Sledování výkonnostních parametrů sítí je zajišťováno nástrojem HP Network Control Center. Tento nástroj je v gesci Oddělení správy sítí.

2.2 Standard pro monitoring HW a OS

2.2.1 Standard pro monitoring UNIX serverů

Pomocí nástroje HP OpenView Operations Manager for Unix (HP OMU) je sledován průběžný stav a výkon všech unixových systémů, které zajišťují provoz aplikací. U klíčových unixových systémů je pro detailnější sledování výkonnosti nasazen HP OpenView Performance Manager.

V prostředí VZP je zavedena základní sada šablon a sada šablon pro sledování výkonnostních parametrů pro sledování unixových serverů.

Podle potřeby je možno monitoring rozšířit nebo upravit.

2.2.2 Standard pro monitoring Windows systémů

Systémy MS Windows jsou spravovány a monitorovány nástrojem System Center Operations Manager (dále jen SCOM), který je v gesci Oddělení správy Microsoft systémů.

Do HP OMU jsou zprávy integrovány pomocí směrování notifikačního kanálu do integračního skriptu operačního systému. Pro každou aplikaci je vytvořen samostatný skript, do kterého je směrován jeden nebo více notifikačních kanálů.

Tvorbu a úpravu skriptů zajišťuje OCD v součinnosti s OSMS, tvorbu notifikačních kanálů a přiřazení zpráv notifikačním kanálům zajišťuje OSMS.

Aktuální seznam Management Packs standardně implementovatelných na instance sledované prostřednictvím SCOM je dostupný na intranetových stránkách OCD. Z tohoto seznamu je nutné vybrat Management Packs potřebné pro každou instanci a zapsat je do Tabulek OTP pro danou aplikaci.

2.2.3 Standard pro monitoring linux systémů

Na vybraných serverech s OS Linux je nainstalován HP OMU agent.

Systémy s OS Linux, na nichž není nainstalován HP OMU agent, jsou monitorovány nástrojem Nagios, který je v gesci OSOS. Vybrané zprávy z Nagios jsou integrovány do centrální operátorské konzole OCD.

K bez-agentnímu sledování linux systémů lze použít i licence Sitescope, a to v závislosti na důležitosti komponenty ve smyslu klasifikace aplikací, a na aktuální dostupnosti licencí.

2.2.4 Standard pro monitoring ostatních systémů

Ostatními systémy mohou být například UPS, tiskárny nebo podobná zařízení, na která není možné instalovat agenta HP OMU, a zároveň tato zařízení nejsou monitorována jiným systémem, který by bylo možné do HP OMU integrovat.

Aby tato zařízení bylo možné monitorovat, je nutné předat informace o sledovaných stavech a/nebo událostech, a o způsobu, jakým lze tato zařízení sledovat (SNMP, HTTP/HTTPS apod.) Zároveň je nutné zajistit přístup k těmto zařízením, například servisním účtem, a také popsat a zajistit patřičné síťové prostupy.

2.3 Standardy monitoringu Oracle komponent

Oracle komponenty jsou nativně sledovány prostřednictvím agentů Oracle Enterprise Manager / Grid Control.

Integrace zpráv z OEM do centrální konzole HP OMU je zajišťována selektivně pomocí skriptů OS, na něž jsou směrována notifikační pravidla (Advanced Notification Method). Velký důraz je kladen na správné přiřazení zpráv k aplikacím a službám (Service_ID), a také k řešitelským skupinám (databázovým, provozně-aplikačním, unixovým). Pro tento účel byla zpracována interní pravidla tvorby notifikačních pravidel pro integraci zpráv z OEM do HP OMU.

Standardní metriky v OEM jsou rozšířeny o uživatelsky definované metriky (UDM); jejich rozsah a nastavení popisuje interní provozní dokument.

3 Standardy aplikačního monitoringu

Následující odstavce popisují standardizované způsoby aplikačního monitoringu. Není-li možné nasadit aplikační monitoring pomocí zavedených nástrojů, poskytne dodavatel v rámci dodávky aplikace monitorovací nástroj (například skript), jehož výstup lze integrovat do HP OMU standardním způsobem.

3.1 Monitoring služeb

Služby a aplikace, které jsou kritické pro chod VZP, jsou monitorovány pomocí E2E transakcí HP BSM, proto je nutné, aby každá taková aplikace měla implementovánu alespoň jednu striktně čtecí roli, kterou do ní bude přistupovat technologický uživatel.

3.2 Monitoring AQ front

Sledování Oracle Advanced Queues je zajišťováno vytvářením uživatelsky definovaných metrik (UDM) v OEM/GC. Tyto metriky musí vytvořit provozní správce aplikace pro všechny kritické fronty požadavků dané aplikace, včetně nastavení limitů pro maximální přípustné počty požadavků ve frontě a pro nejvyšší přípustné stáří požadavku.

Takto vytvořené metriky musejí být zahrnuty do integračního notifikačního pravidla.

3.3 Monitoring WebServices

Monitoring WebServices je obdobou obecného monitoringu služeb - u HA aplikací je možné nasazení měřených E2E transakcí HP BSM, u aplikací nižších tříd je nasazen monitoring pomocí sond na webová rozhraní aplikací.

Seznam použitých zkratek

Zkratka	Význam
AQ	Advanced queueing, Oracle technologie implementující a rozšiřující JMS
AS	Aplikační server
ASM	Archive and Storage Management
BSM	Business Sevice Management
iAS	Aplikační server firmy Oracle
ICT	Informační a komunikační technologie
IPF	Integrační platforma
ISP	Poskytovatel internetového připojení
OMU	Operations Manager for Unix
OV	Open View
UDM	Uživatelsky definované metriky
OEM/GC	Oracle Enterprise Manager / Grid Control.
SCOM	MS System Center Operations Manager
SPI	Smart-Plugins
HA	High Availability
SNMP	Simple Network Management Protokol
MIB	Management Information Base
RADIUS	Remote Authentication Dial In User Service
GSS	Global Site Selector
OID	Object Identifier
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
HTTP/HTTPS	Hypertext Transfer Protocol/ Hypertext Transfer Protocol Secure
E2E	End-to-end