ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - ÚSEK INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ
Křížová 25, 225 08 Praha 5

Standard management vrstvy

Verze 0.54

Změny:

Datum vydání	Verze	Změna proti předchozí verzi	Změnil (jméno)
22.8.2006	0.53	První draft	Jan Bureš
30.8.2006	0.54	Zapracování připomínek	Jan Bureš

Obsah

1. ÚVOD

Předkládaný standard definuje a vymezuje management zónu cílového stavu prostředí ČSSZ. Management zóna je klíčová vrstva prostředí ČSSZ určená ke správě všech ostatních vrstev a systémů v nich umístěných.

2. POPIS MANAGEMENT VRSTVY

Management zóna je jednou z vrstev celkového infrastrukturního prostředí ČSSZ.

Tato vrstva obsahuje administrativní a monitorovací servery a nástroje, které jsou určené ke správě a dohledu nad systémy ve všech ostatních vrstvách. Monitoring (dohled) zajišťuje sledování jednotlivých komponent systému, zejména řízení dostupnosti a výkonu jednotlivých systémů podle definovaných SLA.

Kromě správy a dohledu celého systému ČSSZ jsou v management zóně umístěny master ITIM a ITAM servery . Tyto master servery se replikují do jednotlivých read-only serverů v ostatních vrstvách cílové architektury ČSSZ.

Vzhledem ke geografické redundanci celého prostředí ČSSZ je management zóna rovněž redundantní. Síťová infrastruktura management zóny je zapojena v módu active – active. Služby management nástrojů, budou v redundantním módu. Podle možností konkrétní aplikace, bude mód active-active, nebo active-pasive (tzn. konfiguraci z obou těchto redundantních lokalit nebude možné provádět současně).

Management vrstva jako jediná má přístup do všech ostatních vrstev. Opačný směr je limitovaný.

Celé prostředí musí být navrženo tak, aby při nedostupnosti management zóny nedošlo k výpadku klíčových aplikací. Přes management vrstvu nesmí protékat žádné klíčové informace, protože tato cesta není garantována.

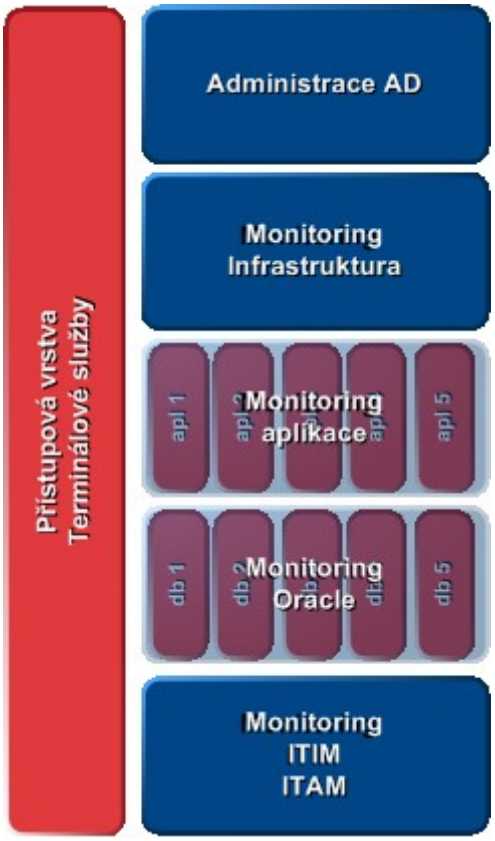
3. SLUŽBY MANAGEMENT VRSTVY

Tato kapitola uvádí přehled konkrétních služeb management vrstvy. Obecně lze tyto služby rozdělit do dvou kategorií – monitoring a administraci.

Management vrstva pro jednotlivé bezpečné vrstvy (proxy, aplikační, databázová) bude plnit následující služby:

- služba přesného času NTP
- jmenné služby DNS
- proxy služby pro přístup do Internetu
- služby automatických aktualizací SUS, depot (unix, linux)

- AD infrastruktura (AD server)



Obr. 3-1 - Schéma služeb management vrstvy – dvě základní funkce – monitoring a administrace

4. MONITORING

Pro potřeby monitoringu prostředí jsou použity dva produkty. Cisco works jako lokální monitoring síťové infrastruktury, a Tivoli, jako monitoring všech komponent IS ČSSZ.

Monitorovaná oblast	Specifikace	Nástroj
Monitoring služeb		
Monitoring infrastrukturních služeb	DNS,WWW	Tivoli
Monitoring serverů	cpu, mem, disk	Tivoli
Monitoring fyzických komponent infrastruktury	SNMP RO, PING, SSH	CiscoWorks
Monitoring UPS	automatic shutdown, no agent	Tivoli
Monitoring prostředí	teplota, vlhkost	
Monitoring služeb databází		Tivoli
Monitoring služeb aplikací		Tivoli
Notifikace, reporting		Tivoli
Vyhodnocování monitoringu		Tivoli
Statistiky služeb	SLA, četnost užití	
Sběr logů z celého prostředí a jejich analýza		
Bezpečnostní monitoring	IDS, IPS	Cisco, MARS (Protego)

4.1 Monitoring Aktivních prvků

Aktivní prvky jsou sledovány pomocí Cisco Works. Jen pomocí tohoto produktu je možné provádět konfiguraci aktivních prvků. Pro přihlášení k aktivním prvkům je použit protokol TACACS. Dohled aktivních prvků je integrován do dohledů Tivoli. Tivoli již nemá žádný přístup k dohledu aktivních prvků.

Použité nástroje:

- Inventory a change management (monitoring) CiscoWorks LMS
- Performance a SLA monitoring CiscoWorks LMS

- Performance monitoring CiscoWorks VMS
- Security monitoring CiscoSecure MARS
- Accounting of administrative tasks CiscoSecure ACS
- Event logging CiscoWorks LMS

Poskytované služby:

- TACACS+ nebo RADIUS
- SYSLOG
- NTP
- SNMP trap destinace
- image repository - TFTP, HTTP, FTP
- CRL repository - LDAP, HTTP

4.2 Monitoring serverů a služeb

Pro monitoring aplikačních serverů je použit produkt Tivoli. Na každém serveru je umístěn agent, který sbírá definované informace a posílá je prostřednictvím Tivoli GW centrální Tivoli consoli. V každé lokalitě je umístěna jedna Tivoli GW, která slouží pro sběr informací v rámci konkrétní lokality. Základní sledované parametry serverů jsou:

- vytížení procesoru
- využití paměti
- volné místo na disku
- klíčové události zapsané do aplikačních logů serverů

Dodavatel každé aplikace, která bude provozovna na aplikačních serverech musí dodat seznam a hodnoty příslušných parametrů, které jsou důležité pro běh vlastní aplikace. Sledování těchto parametrů bude zahrnuto do monitorovacího procesu.

4.3 Monitoring DB Oracle

4.4 Monitoring datového úložiště

4.5 Monitoring IBM HW

Monitoring HW fy IBM bude probíhat pomocí HMC konzole, která bude umístěna v této vrstvě. Tato konzole bude mít přístup do internetu pomocí protokolu HTTPS. Bude odesílat informace přímo výrobci IBM, pro rychlejší odezvu při závadách.

5. ADMINISTRACE

V této kapitole uvádíme přehled jednotlivých administrovaných oblastí systému ČSSZ, jejich specifikaci a konkrétní nástroje, které se v management zóně využívají.

Administrovaná oblast	**Specifikace**	**Nástroj**
Administrace komunikační vrstvy	ssh, https, tftp, no telnet, no html	
Administrace přístupových práv do aktivních prvků		Cisco (tacacs)
Administrace aktivních prvků		Cisco
Administrace HP blade		HP?
Administrace aplikační vrstvy		
Administrace databázové vrstvy		
Administrace ITIM, ITAM, AAA		pomocí www rozhraní
Administrace přístupu z/do externích sítí		
Administrace AD	pomocí vzdálené plochy rdesktop, pouze z management zóny	standardní MS nástroje
Update & upgrade systémů, repository	MS Windows – WSUS Linux - distribuční depot	
Configuration management	konfigurační, binární soubory	

Profylaxe systémů		
Zálohování a obnova dat		
Vyhodnocování logovaných událostí	manuální, předfiltrované, real-time události	

5.1 Administrace aktivních prvků

Administrace aktivních prvků je prováděna pomocí produktu CiscoWorks. Použité protokoly jsou SNMP, FTP, telnet, SSH.

- prikazoveho radku (terminalovym pristup pres console port, SSH nebo telnet)
- CiscoWorks (SSH, telnet, SNMP)
- Cisco Security Manager (SSH)

Tyto produkty slouží také pro distribuci nových verzí a configuration management.

5.2 Administrace AD infrastruktury

Administrace AD bude probíhat prostřednictvím nástrojů fy Microsoft. Tyto nástroje budou umístěny na jednotlivých pracovních stanicích, určených pro přístup do management vrstvy.

5.3 Administrace Oracle DB

Administrace bude probíhat pomocí produktů Oracle

5.4 Administrace aplikačních serverů

5.5 Administrace serverů Blade

Adminustrace Blade serverů bude probíhat pomocí produktu HP

5.6 Administrace IBM produktů

Pro administraci IBM produktů bude v management vrstvě umístěna IBM HMC console. Tato console bude mít přístup do internetu protokolem https, pomocí transparentí proxy, umístěné v management síti.

Budou použity následující produkty:

AIX řádkové rozhraní (CLI) ssh (+ X forwarding)

AIX smitty ssh

AIX scp scp Náhrada ftp

HW pSeries/storage HMC console java klient

HW storage DScli (řádkové rozhraní) ssh

HW storage DS8000 Storage Manager java klient

HW tape library Management páskové knihovny http(s)

FC switche řádkové rozhran (CLI) telnet nelze nahradit ssh

FC switche webové rozhraní http nelze použít https

TSM TSM shell ssh (+ X forwarding) z konzole na TSM server/klient

TSM TSM web zlohovac klient http z konzole na TSM klienta, tenk klient, v případě restore

TSM adminCLI (řádkové rozhraní) vlastní protokol z konzole na TSM server

Oracle Oracle Enterprise Manager http

Oracle sqlplus ssh, sqlnet

Oracle rman ssh, sqlnet

Oracle netca java klient

Oracle dbca java klient

UPS řádkové rozhraní (CLI) telnet nelze nahradit ssh

UPS webové rozhraní http nelze použít https

Tivoli Enterprise Console, Tivoli Monitoring řádkové rozhraní (CLI) ssh

Tivoli Access manager for OS řádkové rozhraní (CLI) ssh

LDAP řádkové rozhraní (CLI) ssh

LDAP webové rozhraní http(s)

6. PŘÍSTUP K NÁSTROJŮM V MANAGEMENT VRSTVĚ

Pro potřeby přístupu k nástrojům management zóny jsou v management vrstvě umístěny pracovní stanice. Použití těchto nástrojů je možné realizovat pouze z těchto stanic. Administrační nástroje jsou dostupné z celého prostředí ČSSZ, Přístup je realizován pomocí

protokolu rdp jen na konkrétní pracovní stanici v management vrstvě. Z této stanice je potom prováděna samotná administrace.

Pro dohled celého prostředí je WWW rozhraní produktu Tivoli vypublikováno do celé sítě ČSSZ.

7. KOMUNIKACE MANAGEMENT VRSTVY S OSTATNÍMI VRSTVAMI

Tato vrstva je jedinou v celé infrastruktuře ČSSZ, která má neomezený přístup do všech ostatních vrstev. Opačná komunikace z libovolné vrstvy směrem do management zóny je však značně limitovaná. Zprostředkování komunikace mezi dvěmi dalšími vrstvami je vyloučená. Komunikace na rozhraní je filtrovaná a monitoruje se pomocí IDS/IPS.

8. ZÁVĚR

Tento dokument definuje a vymezuje management zónu cílového stavu prostředí