ČESKÁ SPRÁVA SOCIÁLNÍHO ZABEZPEČENÍ
ÚSTŘEDÍ - ÚSEK INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

Křížová 25, 225 08, Praha 5

# Standard systémové konfigurace aplikačních serverů

Verze 0.41

**Změny:**

| Datum vydání | Verze | Změna proti předchozí verzi | Změnil (jméno) |
|---|---|---|---|
| 22.1.2005 | 0.10 | První draft | Jaroslav Maurenc |
| 22.1.2005 | 0.11 | Rozšíření požadavků na instalovaný SW | Jiří Brambůrek |
| 22.1.2005 | 0.12 | Doplnění podrobných požadavků na Windows servery | Jiří Sklepník |
| 10.11.2008 | 0.13 | zapracování připomínek | Tomáš Čmakal |
| 11.12.2009 | 0.14 | Aktualizace | Jan Hampl |
| 13.10.2011 | 0.15 | Doplnění | Jan Strnad, Jan Ševčík, Ondřej Dvořák |
| 4.2.2013 | 0.2 | Zapracovaná dlouhodobá strategie ČSSZ | Jan Strnad |
| 4.3.2013 | 0.21 | Zapracován RedHat 6.4 Linux a Windows 2012 | Jan Strnad |
| 5.4.2013 | 0.22 | Zapracování připomínek | Jan Strnad |
| 17.10.2013 | 0.23 | Doplnění | Jan Strnad |
| 25.10.2013 | 0.3 | Zapracování standardizace virtuálního prostředí | Jan Strnad |
| 29.10.2013 | 0.31 | Zapracování synchronizace času | Jan Strnad |
| 30.10.2013 | 0.32 | Zapracování aktualizačního procesu | Jan Strnad |
| 31.10.2013 | 0.33 | Zapracování SNMP | Jan Strnad |
| 1.11.2013 | 0.34 | Zapracování hesel, účtů | Jan Strnad |
| 2.11.2013 | 0.4 | Zapracování sítí a application status | Jan Strnad |
| 26.6.2015 | 0.41 | Zapracování změn | Jan Strnad |

## Obsah


1. ÚVOD ..... 4
   1.1 NOVÉ APLIKACE ..... 4

2. SERVERY MICROSOFT WINDOWS ..... 5
   2.1 Fyzické servery ..... 5
      2.1.1 Konfigurace ..... 5-7
      2.1.2 Instalace z médií ..... 7
      2.1.3 Instalace z image ..... 7-8
      2.1.4 Aktualizace ..... 9-10
   2.2 Virtuální servery ..... 11
      2.2.1 Konfigurace ..... 11-12
      2.2.2 Instalace z médií ..... 13
      2.2.3 Instalace z template ..... 13
      2.2.4 Aktualizace ..... 14-15

3. SERVERY LINUX & VMWARE (ESXI) ..... 16
   3.1 Fyzické servery Linuxem a WMvare ..... 16
      3.1.1 Servery SuSe LINUX ..... 16
      3.1.2 Servery RedHat LINUX ..... 16
      3.1.3 Servery VMware ..... 16
         3.1.3.1 Konfigurace ..... 16-17
         3.1.3.2 Instalace z médií ..... 17
         3.1.3.3 Instalace z image ..... 17
         3.1.3.4 Aktualizace ..... 17

   3.2 Virtuální Servery Linux ..... 18
      3.2.1 CentOS Linux ..... 18
         3.2.1.1 Konfigurace ..... 18
         3.2.1.2 Instalace z médií ..... 18
         3.2.1.3 Instalace z template ..... 18-19
         3.2.1.4 Aktualizace ..... 19
      3.2.2 RedHat Linux ..... 19
         3.2.2.1 Konfigurace ..... 19
         3.2.2.2 Instalace z médií ..... 19
         3.2.2.3 Instalace z template ..... 19-20
         3.2.2.4 Aktualizace ..... 20

4. NASTAVENÍ VIRTUÁLNÍHO PROSTŘEDÍ ..... 21
   4.1 Datové centrum KP1 ..... 22
      4.1.1 Integrace ..... 22
      4.1.2 Test ..... 23
      4.1.3 Produkce ..... 23
      4.1.4 ESB_Backend ..... 24
   4.2 Datové centrum KP2 ..... 25
      4.2.1 Integrace ..... 25
      4.2.2 Test ..... 25
      4.2.3 Produkce ..... 26

5. ČASOVÁ SYNCHRONIZACE ..... 27
6. PRINCIP AKTUALIZACÍ V APLIKAČNÍ VRSTVĚ.....28
6.1 WSUS ..... 28
6.2 Linux repository..... 29
6.3 VMware ..... 30

7.SNMP..... 32

8. TVORBA HESEL, ÚČTY A JEJICH PRAVIDLA..... 37

9. SÍŤOVÁ INFRASTRUKTURA APLIKAČNÍ VRSTVY..... 38

10. KEEP A LIVE URL / APPLICATION STATUS ..... 40

11. ZÁVĚR..... 41

# 1. ÚVOD

Cílem dokumentu je specifikovat standard konfigurace aplikačních serverů a prostředí v ČSSZ. Standardizována je konfigurace následujících systémů aplikačních serverů

- Microsoft Windows Server 2003 (stále se provozuje i přes ukončení podpory výrobce, již není instalován pro nové aplikace, pouze do doby převodu na nové OS Windows 2012 R2)
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7
- Suse Linux
- RedHat Linux
- Cent OS Linux
- VMware (logické řazení a obecná nastavení prostředí)
- Aktualizace
- Časová synchronizace
- Tvorba a pravidla hesel, účtů a jejich pravidla

Instalaci a konfiguraci jiných než výše uvedených systémů musí projednat a schválit provozní porada.

## 1.1 NOVÉ APLIKACE

Pro nové aplikace budou instalovány pouze OS ve virtuálním prostředí:

- **Microsoft Windows Server 2008 R2**
- **Microsoft Windows Server 2012 R2**
- **Microsoft Windows 7**
- **Linux CentOS 6.X (x64) a novější**
- **Linux RedHat 6.X (x64) a novější**
- **Linux CentOS 7.X (x64) a novější**
- **Linux RedHat 7.X (x64) a novější**

# 2. SERVERY MICROSOFT WINDOWS

## 2.1. FYZICKÉ SERVERY MICROSOFT WINDOWS

Na servery jsou instalovány následující operační systémy v anglické verzi

- Microsoft Windows Server 2003 Standard Edition 32bit + SP2
- Microsoft Windows Server 2008 Enterprise Edition x64
- Microsoft Windows Server 2008 Standard Edition 64bit + SP2
- Microsoft Windows Server 2008 R2 Standard Edition 64bit
- Microsoft Windows Server 2012 Standard Edition 64bit

### 2.1.1 KONFIGURACE

Výchozí konfigurace:

Základ aplikačních serverů na ČSSZ je tvořen farmami blade serverů, které jsou umístěné v lokalitách KP1 a KP2 a sestávají z několika typů:

Typ BL20p – servery sa1x001 až sa1x100, sa2x001 až sa2x100 – 2 x procesor Xeon 3.2 GHz, 4 GB RAM, 2x 72 GB HD (pouze dosluhují)

Typ BL460c – servery sa1x101 až sa1x134, sa2x101 až sa2x134 – 2 x procesor Xeon 2.66 GHz 2-jádrový, 8 GB RAM, 2x 72 GB HD + Rozšíření RAM

Typ BL460c – servery sa1x135 až sa1x146, sa2x135 až sa2x146 – 1 x procesor Xeon 2.66 GHz 4-jádrový, 8 GB RAM, 2x 72 GB HD + Rozšíření RAM

Typ BL680c – servery sa1x149 až sa1x156, sa2x149 až sa2x156 – 4 x procesor Xeon 2.66 GHz 6-jádrový, 32 GB RAM, 2x 72 GB HD + Rozšíření RAM

- Servery jsou konfigurovány tak, že mají celý disk naformátován jako jedinou partition, tj. pouze disk C. Logický disk je tvořen minimálně 2 fyzickými disky v poli RAID1.
- Na servery je možné nainstalovat všechny aktuálně dostupné otestované záplaty OS. Ty jsou přebírány z centrálního WSUS serveru na WSUS servery, nainstalované na DC domén app.cssz.cz a i-app.cssz.cz.
- Na servery je podle potřeby aplikací možno instalovat následující systémový SW:

| Poř. Číslo | Název aplikace či komponenty | Poznámka |
|---|---|---|
| **1** | IIS (ASP, ASP.NET, FTP, SSI) | Systémová komponenta – verze dle použitých OS |
| **2** | Klient Antivir | Instaluje se na každém serveru v doméně app.cssz.cz a i-app.cssz.cz |
| **3** | Management SW (Tivoli End Point) | |
| **4** | Microsoft .NET Framework | V případě potřeby možno instalovat jako součást systému W2003 ve verzi 1.1, lze aktualizovat přes WSUS na 2.0 a 3.0 nebo 3.5 atd.. , u W2008 lze doinstalovat jako Features ve verzi 3.0 u W2008 R2 také jako Features ve verzi 3.5.1 a vyšší ( 4.0, 4.5, …) |
| **5** | Nagios klient | Klient kompatibilní s NAGIOSEM používaný na oddělení monitoringu |
| **6** | Microsoft Windows Installer 3.1 a vyšší | |
| **7** | Microsoft SQL Server Native | |
| **8** | WebDeploy | |
| **9** | Microsoft XML Core Services 6.0 a vyšší | |
| **10** | Microsoft Windows PowerShell 2.0 a vyšší | Systémová komponenta pro Windows Server 2008 |
| **11** | Oracle client 9.2 a 10.2 a 11g a 12c<br>Oracle X ODAC (Oracle Data Access Components) | Pouze u specializovaných serverů, kde je to vyžadováno aplikací |

Základní konfigurace serveru je následující:

- IP adresace dle umístění/aplikace serveru
- Nastavení synchronizace času (doménové kontrolery, PDC emulátory přebírají čas od NTP serveru 10.11.47.10 )
- Povolení vzdáleného přístupu (RDP)
- Nastavení antivirového SW
- Nastavení management SW
- Nastavení automatických aktualizací (např. pomocí WSUS potažmo GPO v AD politikou nebo lokální politikou)

## 2.1.2 INSTALACE Z MÉDIÍ

- Instalaci popřípadě přeinstalaci operačních systémů na serverech obou bladových farem provádí zaměstnanci Oddělení správy datových úložišť ústředí ČSSZ (dále jen „odd. 524"), produktem RDP z předpřipravených a schválených image na fyzických serverech.
- Z médií byl doposud instalován firmou Microsoft pro potřebu BizTalk OS Microsoft Windows Server 2003 Enterprise Edition x64 SP2, který se již na blade serverech nevyskytuje. Co se týče Microsoft Windows Server 2008 Enterprise Edition x64, ty jsou použity pro potřebu BizTalk a již jsou také na ústupu.
- Dále na doménových kontrolerech domén app.cssz.cz a i-app.cssz.cz byl proveden upgrade OS na Microsoft Windows Server 2008 R2.
- Nyní jsou připraveny image operačních systémů Windows uvedených v bodě 2.1.3 pro jednotlivé typy bladových serverů.

## 2.1.3 INSTALACE Z IMAGE

- Operační systémy jsou na požadované servery instalovány z předem připravených, schválených a otestovaných image produktem Rapid Deployment Pack, který je umístěn na řídících serverech HP DL360 G4 /jeden v každé lokalitě/.
- Image /verze 1/ níže uvedených operačních systémů pro původní dodávku bladů /typ BL20p G3/ zpočátku vytvářela firma HP, poté upravovala a nové image vytvářela firma Alwil:

1) W2003 Server standard edition, SP2, eng.
2) W2003 Server R2 Standard Edition 32bit + SP2,eng. S IIS + .NET
3) W2003 Server R2 Standard Edition 32bit + SP2
4) W2008 Server standard edition 64 bit eng.
5) W2008 R2 std.
6) Linux SUSE 9.3
7) RedHat v.4

Pro pozdější dodávku bladů BL460c image /verze 2/ vytvářela firma Alwil.

Pro tyto blade servery jsou připraveny následující image:

1) W2003 Server Standard Edition, SP2, eng.
2) W2003 Server Standard Edition, SP2, eng., a dále s IIS + .NET
3) W2003 Server R2 Standard Edition 32bit + SP2,eng. S IIS + .NET
4) W2003 Server R2 Standard Edition 32bit + SP2
5) W2008 Server Standard Edition 64 bit, eng.
6) W2008 R2 std.
7) Linuxová image pro OS Linux SUSE 10.1

Požadavek na vytvoření image OS RedHat pro blady BL460c nebyl.

Pro novější dodávku bladů BL680c vytvářela image (verze 3) rovněž firma Alwil.

Pro tyto blade servery jsou připraveny následující image:

1) W2008 Server Standard Edition 64 bit, eng.

2) W2008 Server R2 Standard Edition 64 bit, eng.

Požadavek na vytvoření image Windows 2003, Windows 2003 R2, OS RedHat a Linux SUSE pro blady BL680c nebyl.

Bude-li požadavek na vytvoření image dalších OS, je toto zajištěno v rámci smluvního vztahu o podpoře bladových farem s firmou Alwil (ve spolupráci s odd. 524).

- Vlastní instalace operačního systému je prováděna z řídících konzolí (servery HP DL360 G4 ), které jsou ve stejné síti 10.200.20.y v lokalitě KP1 nebo 10.201.20.y v lokalitě KP2 jako farmy blade serverů. Na této konzoli je spuštěn produkt RDP, volbou *Job scheduling Wizard* je nadále vyhledán již vytvořený job pro deployment image operačního systému na zvolený server. Vlastní image obou operačních systémů se nalézají na disku C:\Program Files\ Altiris\eXpress\Deployment Server\Images. V dalším postupu je nutno potvrdit znovu server, na který se má OS nahrát, aby nedošlo k přeinstalaci jiného serveru. Poté je nabídnuta možnost spustit job ihned nebo později. Po spuštění jobu již vše probíhá samočinně, server je několikrát restartován během tohoto procesu.
- Po nahrání OS jsou serveru přiděleny IP adresy od DHCP. Blade servery mají 4 síťové karty, fyzicky propojené do aktivních prvků jsou pouze 2 / až na výjimky – servery pro BT2006 a některé servery pro AAA portál, kde jsou zapojeny všechny 4 síťové karty/. Ty jsou poté nastaveny do teamingu, v případě výpadku jedné přebírá komunikaci druhá. Pak je nutné pro tento tým nastavení skutečné IP adresy:

    1. standardně na adresy 10.200.20.y nebo 10.201.20.y podle lokality,
    2. podle aplikace a VLAN, do které je aplikace zařazena, zařazení do VLAN je prováděno požadavkem na HP přes tzv. provisioning. Zde je nastavován při instalaci OS a aplikace stav Install, po doinstalaci aplikace možno změnit stav na Active /load balancing/. (Metody rozkladu zátěže: Round-robin, Least connections)
    3. následuje nahrání klienta pro komunikaci s UPS, kde je nutno zadat IP karty v UPS, přes kterou je komunikace zprostředkovávána,
    4. pokud je požadavek, je server zařazen do domény app.cssz.cz/ nebo i-app.cssz.cz/, nastaveno DNS, nahrán antivirový program, server je rovněž zařazen do příslušného OU na doménovém controleru. Je také určen X_Admin/X_Operátors pro aplikaci a vytvořen příslušný účet. Do domény app.cssz.cz /i-app.cssz.cz/ budou postupně zařazovány všechny blady servery.
    5. Regionální nastavení: CZECH

       Lokalizace: CZ

       Klávesnice: US + CZ

Tento model se pomalu opouští, jelikož se vše přenáší na virtualizační platformu.

### 2.1.4 AKTUALIZACE

- Případné stažení záplat na OS bude nejdříve testováno v integračním prostředí a je na správě aplikací, jaké aktualizace je možno z WSUSU stáhnout, aby aplikace nebyly ohroženy.
- Záplaty jsou nabízeny pomocí automatických aktualizací, správci serverů mají možnost výběru z nabízených záplat. Aktualizace jsou přejímány z centrálního WSUS serveru na WSUS servery v doménách APP a i-APP.
- U serverů a stanic nezařazených do domén APP a i-APP je nutno nakonfigurovat napojení na WSUS server pomocí lokálních politik:

spuštěním příkazu **gpedit.msc** otevřeme z nabídky *Start, dále Šablony pro správu, Součásti systému Windows, Windows Update, popř. Computer Configuration, Administrative Templates,Windows Components, Windows Update*

Bližší informace o aktualizacích WSUS v kapitole 6.1.

Nastavení lokálních politik je uvedeno v následující tabulce (Produkce):

| | |
|---|---|
| Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box | Not configured |
| Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box | Not configured |
| Configure Automatic Updates | Enabled<br>2. Notify download and notify to install<br>0 – Every Day<br>Install time:03:00 |
| Specify intranet Microsoft update service location | Enabled<br>Update service: http:// 10.200.200.180<br>Statistic server: http://10.200.200.180 |
| Enable client-side targeting | Enabled<br>Targed group: *TECHSITPC_APP pro PC nebo TECHSITSER_APP pro servery* |
| Reschedule Automatic Updates scheduled installations | Not configured |
| No auto-restart for scheduled Automatic Updates | Enabled |
| Automatic Updates detection frequency | Enabled<br>10 |
| Allow Automatic Updates immediate installation | Not configured |
| Delay Restart for scheduled installations | Not configured |
| Re-prompt for restart with scheduled installations | Not configured |
| Allow non-administrators to receive update notifications | Not configured |
| Enable recommended updates via Automatic Updates | Not configured |
| Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates | Not configured |
| Allow signed content from intranet Microsoft update service location | Not configured |

## 2.2 VIRTUÁLNÍ SERVERY MICROSOFT WINDOWS

Na servery jsou instalovány následující operační systémy v anglické verzi:

- Microsoft Windows Server 2000 Standard Edition 32bit
- Microsoft Windows Server 2003 Standard Edition 32bit + SP1
- Microsoft Windows Server 2003 Standard Edition 32bit + SP2
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7

### 2.2.1 KONFIGURACE VIRTUÁLNÍCH SERVERŮ MICROSOFT

Výchozí konfigurace:

- Virtuální aplikační servery v ČSSZ jsou v podstatě jediného typu (co se týče virtuálního HW). Standard byl stanoven s těmito parametry:

  Typ virtuální server VMware – 1 x CPU nebo 4 x jádro, 4GB RAM, 40GB, dle požadavku lze přidat, jak CPU, RAM, tak HDD.

- Servery jsou v základu konfigurovány tak, že mají jeden HDD o velikosti 40 GB s jedinou partition , tj. pouze disk C. U serverů je pouze jeden HDD pro OS, další HDD by měly být buď síťové nebo RDM. Na aplikačních serverech se nesmějí vyskytovat data!

- Na servery je možné nainstalovat všechny aktuálně dostupné otestované aktualizace OS. Ty jsou přebírány z centrálního WSUS serveru na WSUS servery, nainstalované na DC domén app.cssz.cz a i-app.cssz.cz.

- Na servery je podle potřeby aplikací možno instalovat následující systémový SW:

| Poř. Číslo | Název aplikace či komponenty | Poznámka |
|---|---|---|
| **1** | IIS (ASP, ASP.NET, FTP, SSI) | Systémová komponenta – verze dle použitého OS |
| **2** | Klient Antivir | Instaluje se na každém serveru v doméně app.cssz.cz a i-app.cssz.cz |
| **3** | Management SW (Tivoli EndPoint) | |
| **4** | Microsoft .NET Framework | V případě potřeby možno instalovat jako součást systému W2003 ve verzi 1.1, lze aktualizovat přes WSUS na 2.0 a 3.0 anebo 3.5 atd.. , u W2008 lze doinstalovat jako Features ve verzi 3.0 u W2008 R2 také jako Features ve verzi 3.5.1 a vyšší ( 4.0, 4.5, …) |
| **5** | Nagios klient | Klient kompatibilní s NAGIOSEM používaný na oddělení monitoringu |
| **6** | Microsoft Windows Installer 3.1 a vyšší | |
| **7** | Microsoft SQL Server Native | |
| **8** | WebDeploy | |
| **9** | Microsoft XML Core Services 6.0 a vyšší | |
| **10** | Microsoft Windows PowerShell 2.0 a vyšší | Systémová komponenta pro Windows Server 2008 |
| **11** | Oracle client 9.2, 10.2, 11g a 12c<br>Oracle X ODAC (Oracle Data Access Components) | Pouze u specializovaných serverů, kde je to vyžadováno aplikací |

Základní konfigurace serveru je následující:

- IP adresace dle umístění/aplikace serveru
- Nastavení synchronizace času (doménové kontrolery, PDC emulátory přebírají čas od NTP serveru 10.11.47.10 )
- Povolení vzdáleného přístupu (RDP)
- Nastavení antivirového SW
- Nastavení management SW

- Nastavení automatických aktualizací (např. pomocí WSUS potažmo GPO v AD politikou nebo lokální politikou)

### 2.2.2 INSTALACE Z MÉDIÍ

- Instalaci, popřípadě reinstalaci operačních systémů na virtuálních serverech na obou lokalitách, provádí zaměstnanci odd. 524 pomocí VMware.
- Dále na doménových kontrolerech domén app.cssz.cz a i-app.cssz.cz byl proveden z instalačních médií upgrade OS na Microsoft Windows Server 2008 R2. Tyto doménové kontrolery jsou již virtuální. Upgrade OS na vyšší verze u doménových kontrolerů probíhá nejdříve v doméně i-app.cssz.cz a po minimálně šesti měsících i na app.cssz.cz

### 2.2.3 INSTALACE Z TEMPLATE

- Virtuální servery jsou instalovány z připravených template, vytvořených dle požadavku na provoz aplikací. Operační systémy/virtuální servery jsou instalovány z předem připravených template, schválených a otestovaných. Instalace se provádí z VCenter serverů.

Přehled template:

1) W2000_SP2 – pouze pro aplikaci CACNODE která se převedla z 10.6.x.y do apl. vrstvy
2) W2003_SP2_NO_IIS
3) W2003_SP1 – kvůli zpětné kompatibilitě starých aplikací viz převod aplikací ze sítě 10.6.x.y
4) W2003_SP2
5) W2003_SP2_ATOS - Předpřipravené instalační skripty
6) W2003_KE2 - Předpřipravené instalační skripty pro KE2
7) W2008_R2_Standart
8) W2008_R2_Enterprise
9) W2012
10) W7

- Vlastní instalace operačního systému je prováděna z VCenter serveru z předdefinovaných template, při instalaci lze měnit jednotlivé HW parametry.
- Během instalace je nastavena příslušná IP adresa a VLAN, virtuální stroj má jednu síťovou kartu.
- Síťové rozhraní je nastaveno podle aplikace a VLAN, do které je aplikace zařazena, zařazení do VLAN je prováděno požadavkem na HP přes tzv. provisioning. Zde je nastavován při instalaci OS a aplikace stav Install, po doinstalaci aplikace možno změnit stav na Active /load balancing/. (Metody rozkladu zátěže: Round-robin,Least connections)
- Pokud je požadavek, je server zařazen do domény app.cssz.cz/ nebo i-app.cssz.cz/, nastaveno DNS, nahrán antivirový program, server je rovněž zařazen do příslušného OU na doménovém kontroleru. Je také určen X_Admin/X_Operátors pro aplikaci a

vytvořen příslušný účet. Do domény app.cssz.cz /i-app.cssz.cz/ budou postupně zařazovány všechny servery.

### 2.2.4 AKTUALIZACE

- Případné stažení aktualizací na OS bude nejdříve testováno v integračním prostředí a je na správě aplikací, jaké aktualizace je možno z WSUSu v dalších prostředích stáhnout, aby aplikace nebyly ohroženy.
- Záplaty Aktualizace jsou nabízeny pomocí automatických aktualizací, správci serverů mají možnost výběru z nabízených aktualizací. Aktualizace jsou přejímány z centrálního WSUS serveru na WSUS servery v doménách APP a i-APP.
- U serverů a stanic nezařazených do domén APP a i-APP je nutno nakonfigurovat napojení na WSUS server pomocí lokálních politik:

spuštěním příkazu **gpedit.msc** otevřeme z nabídky *Start, dále Šablony pro správu, Součásti systému Windows, Windows Update, popř. Computer Configuration, Administrative Templates,Windows Components, Windows Update*

Bližší informace o aktualizacích WSUS v kapitole 6.1.

Informace o stahovaných aktualizacích budou zřejmě uvedeny v standardu odd 523,náš WSUS server je podřízený jejich.

Nastavení lokálních politik je uvedeno v následující tabulce (Produkce):

| | |
|---|---|
| Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box | Not configured |
| Do not adjust default option to 'Install Updates and Shut Down' in Shut Down Windows dialog box | Not configured |
| Configure Automatic Updates | Enabled<br>2. Notify download and notify to install<br>0 – Every Day<br>Install time:03:00 |
| Specify intranet Microsoft update service location | Enabled<br>Update service: http:// 10.200.200.180<br>Statistic server: http://10.200.200.180 |
| Enable client-side targeting | Enabled<br>Targed group: *TECHSITPC_APP pro PC nebo TECHSITSER_APP pro servery* |
| Reschedule Automatic Updates scheduled installations | Not configured |
| No auto-restart for scheduled Automatic Updates | Enabled |
| Automatic Updates detection frequency | Enabled<br>10 |
| Allow Automatic Updates immediate installation | Not configured |
| Delay Restart for scheduled installations | Not configured |
| Re-prompt for restart with scheduled installations | Not configured |
| Allow non-administrators to receive update notifications | Not configured |
| Enable recommended updates via Automatic Updates | Not configured |
| Enabling Windows Update Power Management to automatically wake up the system to install scheduled updates | Not configured |
| Allow signed content from intranet Microsoft update service location | Not configured |

# 3. SERVERY LINUX &VMWARE (ESXI)

## 3.1.1 FYZICKÉ SERVERY S LINUXEM A WMVARE

## 3.1.1 SERVERY SUSE LINUX

- Operační systém Linux *SUSE 9.3 a* Linux *SUSE 10.1* je obdobně jako operační systémy Windows instalován z image vytvořené pro rozinstalovávání tohoto OS na požadované servery. Opět je využíváno produktu Rapid Deployment Pack. Image byla vytvořena pro potřebu některých aplikací na základě požadavku a po otestování firmou SBS /SITSS/ATOS.
- V případě OS Linux SUSE nastavení teamingu síťových karet a mirroringu HDD provádí administrace aplikací.
- Tento operační systém je již postupně nahrazován a CentOS na virtuálním prostředí.

## 3.1.2 SERVERY REDHAT LINUX

- Na části aplikačních serverů pro AAA portál /WebSealy/ je OS Linux RedHat. Image pro tento OS máme jen pro původní dodávku serverů BL20p G3. Image byla vytvořena pro potřebu aplikací AAA na základě požadavku a po otestování firmou SBS /SITSS/ATOS.
- Postup instalace operačního systému RedHat produktem Rapid Deployment Pack je shodný jako postup při instalaci OS Windows.
- V případě OS Linux SUSE nastavení teamingu síťových karet a mirroringu HDD provádí administrace aplikací.
- Tento operační systém je již postupně nahrazován systémem RedHat ve virtuálním prostředí.

## 3.1.3 SERVERY WMVARE (ESXI)

Servery s hypervizory ESXI jsou instalovány na nové blade servery BL 685c G7.
Jsou děleny do standartních prostředí Integrace, Test, Produkce.

### 3.1.3.1 KONFIGURACE

Výchozí konfigurace:

- Fyzické stroje pro virtualizační platformu v ČSSZ jsou tvořeny farmami blade serverů BL 685c G7, které jsou umístěné v lokalitách KP1 a KP2:

  Typ BL685 – servery sa1x157 až sa1x180, sa2x157 až sa2x180 – 4 x procesor AMD 2,6 GHz / 8 jader, min 64 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /

- Servery jsou konfigurovány tak, že mají celý disk naformátován jako jedinou partition , tj. pouze disk C. Logický disk je tvořen minimálně 2 fyzickými disky v poli RAID1. U serverů dodaných bez HDD je v serveru paměť typu flash na které je nainstalován hypervizor (ESXI) cca 400MB

- Na servery je možné nainstalovat všechny aktuálně dostupné otestované záplaty ESXI. Ty jsou přebírány z VCenter serveru, kam jsou dodávány formou balíčků, které jsou manuálně stahovány za internetu. Více v kapitole 6.3.

Základní konfigurace serveru je následující:

- IP adresace dle umístění serveru
- Nastavení synchronizace času / doménové kontrolery přebírají čas od NTP serveru 10.11.47.10 /

### 3.1.3.2 INSTALACE Z MÉDIÍ

- Instalaci popřípadě přeinstalaci/reinstalaci se provádí pomocí instalačního media či ISO image.
- Časová náročnost je cca 30 – 60 min.
- Aktualizace se provádí z VCenter serveru.

### 3.1.3.3 INSTALACE Z IMAGE

- Není požadována, instalace se provádí pouze z medií.

### 3.1.3.4 AKTUALIZACE

Import a následnou instalaci nových aktualizací provádějí zaměstnanci odd. 524.

Postup:

1) Import příslušné aktualizace do VCenter serveru + vytvoření Job
2) Aktualizace hypervizoru (ESXI)
3) Aktualizace VM, většinou se jedná o celé verze
4) Aktualizace VMTOOLS, v příslušných VM

## 3.2 VIRTUÁLNÍ SERVERY S LINUXEM

### 3.2.1 SERVERY CENTOS LINUX

- Operační systém CentOS 6.X a CentOS 7.X ( Linux ) byl primárně požadován kvůli sjednocení OS Linux. Byla vybrána platforma CentOS, která je bitově kompatibilní s RedHat Enterprise Linux, potažmo Oracle Linux (jedná se o odvozeninu z RedHat Enterprise Linux jako je CentOS).

#### 3.2.1.1 KONFIGURACE

Výchozí konfigurace:

- Virtuální aplikační servery v ČSSZ jsou v podstatě jediného typu (co se týče virtuálního HW). Standard byl stanoven s těmito parametry:

  Typ virtuální server VMware – 1 x CPU nebo 4 x jádro, 4GB RAM, HDD1: 20GB a HDD2: 20GB dle požadavku lze přidat, jak CPU, RAM tak HDD.

- Servery jsou v základu konfigurovány tak, že mají dva HDD o velikosti 20 GB pro OS a další HDD by měli být buď síťové nebo RDM.
- Na serverech bude provozována JAVA a aplikace nativní pro Linux např. Apache, PHP, atd.…
- Na serverech CentOS budou provozovány pouze stabilní aplikace.
- CentOS bude nativně startovat do textového režimu.
- Defaultně bude povoleno SSH popřípadě VNC pro oprávněné uživatele.
- Na serverech budou účty pro administraci aplikací a doménové správce (APP/I-APP).
- Jednotná správa OS Linux bude řešena později.

#### 3.2.1.2 INSTALACE Z MÉDIÍ

- Instalaci popřípadě přeinstalaci/reinstalaci operačních systémů na virtuálních serverech obou lokalitách provádí zaměstnanci odd. 524, pomocí VMware.

#### 3.2.1.3 INSTALACE Z TEMPLATE

- Virtuální servery jsou instalovány z připravených template. Operační systémy/virtuální servery jsou instalovány z předem připravených template, schválených a otestovaných. Instalace se provádí z VCenter serverů.

Přehled template:

1) CENT_OS_6.2_FINAL

- Vlastní instalace operačního systému je prováděna z VCenter serveru z předefinovaných template, při instalaci lze měnit jednotlivé HW parametry.

- Během instalace je nastavena příslušná IP adresa a VLAN, virtuální stroj má jednu síťovou kartu.
- Síťové rozhraní je nastaveno podle aplikace a VLAN, do které je aplikace zařazena, zařazení do VLAN je prováděno požadavkem na HP přes tzv. provisioning. Zde je nastavován při instalaci OS a aplikace stav Install, po doinstalaci aplikace možno změnit stav na Active /load balancing/. (Metody rozkladu zátěže: Round-robin,Least connections)
- Takto předpřipravený OS je minimální instalací 64-bit OS + mc, nmtui a VMTools

#### 3.2.1.4 AKTUALIZACE

- Aktualizace tohoto OS se bude řešit buď systémovým řešením v rámci celé ČSSZ (kaskádovým řetězením serverů Rsync + Proxy.

### 3.2.2 SERVERY REDHAT LINUX

- Operační systém RedHat 6.X Enterprise nebo RedHat 7.X Enterprise ( Linux ) je požadován kvůli AAA WS serverům nebo iMC.

#### 3.2.2.1 KONFIGURACE

Výchozí konfigurace:

- Virtuální aplikační servery v ČSSZ jsou v podstatě jediného typu (co se týče virtuálního HW). Standard byl stanoven s těmito parametry:

  Typ virtuální server VMware – 4 x CPU nebo 4 x jádro, 4GB RAM, HDD: 40GB dle požadavku lze přidat, jak CPU, RAM tak HDD.
- Servery jsou v základu konfigurovány tak, že mají jeden HDD o velikosti 40 GB pro OS a další HDD by měly být buď síťové nebo RDM.
- Tyto servery jsou takovou speciální skupinou serverů (jedná se o část dodávky SW řešení AAA portálu nebo iMC)
- Na serverech budou účty pro administraci aplikací a doménové správce (APP/I-APP/nebo jiné)
- Jednotná správa OS Linux bude řešena pomocí FreeIPA (již testujeme v pilotním provozu)

#### 3.2.2.2 INSTALACE Z MÉDIÍ

- Instalaci popřípadě přeinstalaci/reinstalaci operačních systémů na virtuálních serverech obou lokalitách provádí zaměstnanci odd. 524, pomocí VMware.

#### 3.2.2.3 INSTALACE Z TEMPLATE

- Virtuální servery jsou instalovány z připravených template. Operační systémy/virtuální servery jsou instalovány z předem připravených template, schválených a otestovaných. Instalace se provádí z VCenter serverů.

Přehled template:

1) RedHat_6.X
2) RedHat_7.X

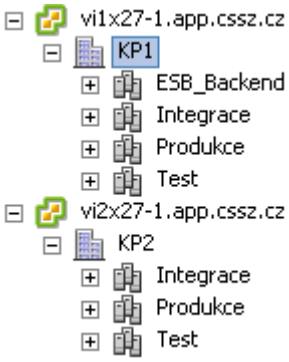
- Vlastní instalace operačního systému je prováděna z VCenter serveru z předefinovaných template, při instalaci lze měnit jednotlivé HW parametry.
- Během instalace je nastavena příslušná IP adresa a VLAN, virtuální stroj má jednu síťovou kartu.
- Síťové rozhraní je nastaveno podle aplikace a VLAN, do které je aplikace zařazena, zařazení do VLAN je prováděno požadavkem na HP přes tzv. provisioning. Zde je nastavován při instalaci OS a aplikace stav Install, po doinstalaci aplikace je možno změnit stav na Active /load balancing/.

#### 3.2.2.4 AKTUALIZACE

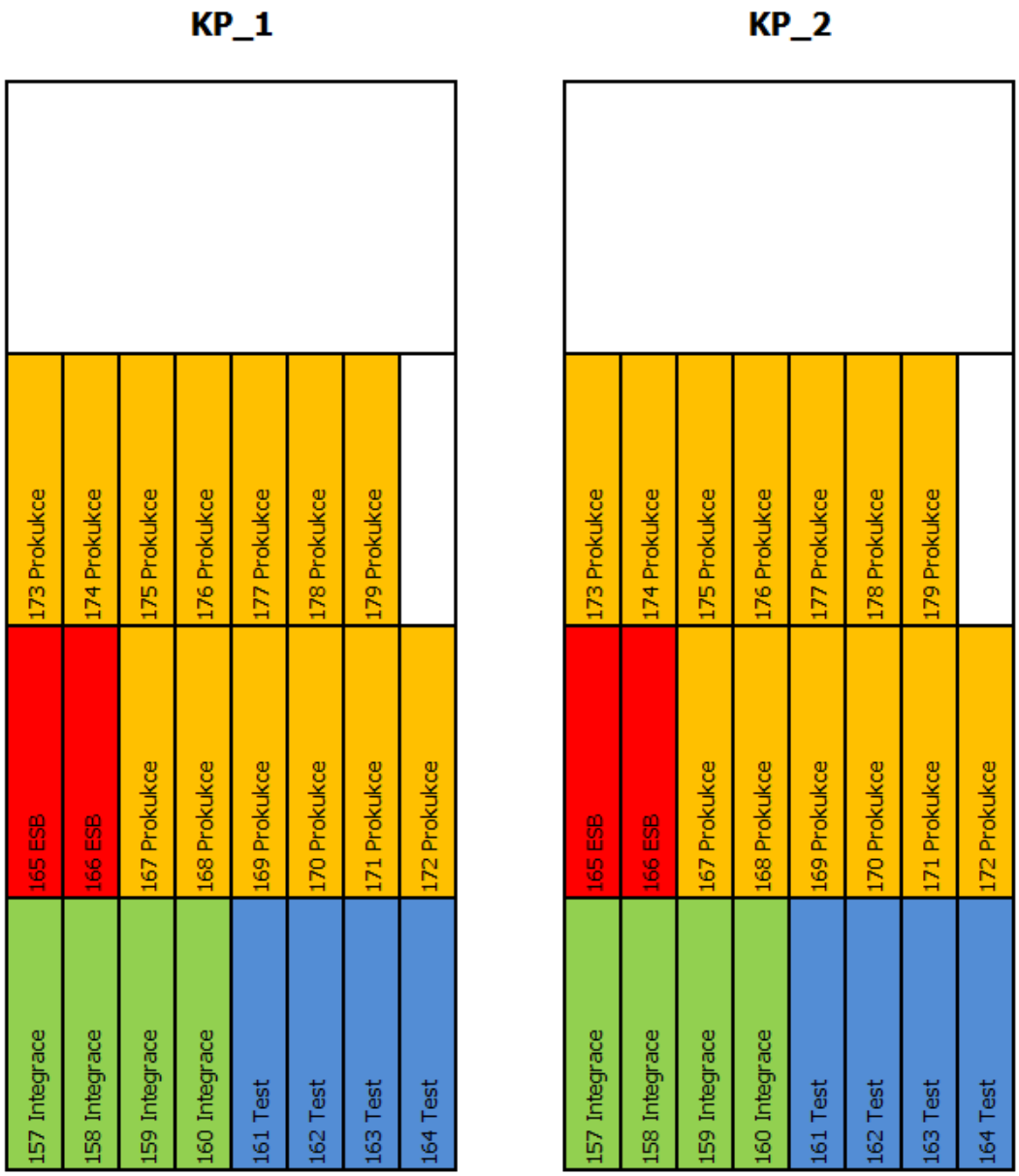
- Aktualizace tohoto OS se bude řešit buď systémovým řešením v rámci celé ČSSZ (kaskádovým řetězením serverů Rsync + Proxy).

# 4. NASTAVENÍ VIRTUÁLNÍHO PROSTŘEDÍ

- Virtuální prostředí v aplikační vrstvě je postaveno bázi VMware v aktuální verzi.
- Verze VMware se aktualizuje vždy 2-3 měsíce po uvedení aktuální verze, nebo ve výjimečných případech se aktualizuje, pokud opravuje závažnou funkční či bezpečností chybu, provádí odd.524
- Virtuální prostředí je v základu rozděleno na dvě části a to dle lokality: KP1 a KP2
    - Tyto lokality jsou reprezentovány tzv. VCener servery, tyto servery jsou centrální managementem pro danou lokalitu (jedná se o virtuální servery). Tyto management servery jsou propojeny (linked mode) a dají se obě lokality spravovat z jedné z nich. Centrální management provádí pracovníci odd.524.
        - Pod každým VCenter serverem je další organizační struktura, která reprezentuje datové centrum v dané lokalitě (KP1 a KP2)
            - Posledním a nejdůležitějším celkem, který se nachází pod datovými centry jsou VMware clustery. Tyto clustery rozdělují virtuální servery do skupin dle prostředí a škálují jejich zdroje a dostupnost v rámci virtuálního prostředí. Tyto vlastnosti jsou dány tímto standardem a zodpovídají za ně pracovníci odd. 524.




Logické řazení v prostředí VMware




Rozložení serverů pro virtualizaci v lokalitách.

## 4.1 DATOVÉ CENTRUM KP1

- Má pod sebou čtyři organizační podsložky, tzv. „VMware Clustery" tyto clustery jsou:
    - Integrace
    - Test
    - Produkce
    - ESB_Backend
- Integrace, Test, Produkce mají stejné nastavení v lokalitě KP1 a v lokalitě KP2. Cluster ESB_Backend je speciální a nachází se v pouze v lokalitě KP1 i když je rozkročen přes obě lokality. Je to z důvodu technického řešení, v této organizační struktuře se nacházejí servery jak z integrace, testu, tak i z produkce a sdílejí mezi sebou zdroje.

### 4.1.1 INTEGRACE

- Integrační prostředí má pro sebe dedikované 4 servery
- Typ BL685 – servery sa1x157 až sa1x160 – 4 x procesor AMD 2,6 GHz / 8 jader, min 128 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Integračního Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - Nastavena redundance N+1
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
        - Power Management: Automatic (se střední hodnotou)

- Tento cluster je nastaven, tak aby poskytoval dostatek výpočetního výkonu pro dané servery i v případě výpadku jednoho z daných serverů. Zároveň je nastaven tak, aby se choval ekonomicky a v případě nevyužitého výkonu převedl daný server do režimu spánku.

### 4.1.2 TEST

- Testovací prostředí má pro sebe dedikované 4 servery
- Typ BL685 – servery sa1x161 až sa1x164 – 4 x procesor AMD 2,6 GHz / 8 jader, min 128 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Testovacího Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - Nastavena redundance N+1
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
        - Power Management: Automatic (se střední hodnotou)

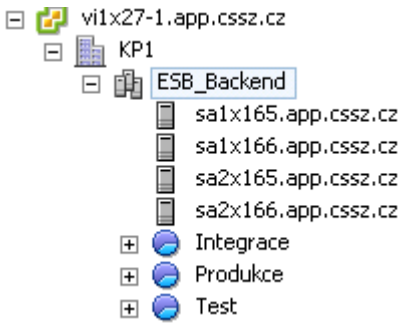
- Tento cluster je nastaven, tak aby poskytoval dostatek výpočetního výkonu pro dané servery i v případě výpadku jednoho z daných serverů. Zároveň je nastaven tak, aby se choval ekonomicky a v případě nevyužitého výkonu převedl daný server do režimu spánku.

### 4.1.3 PRODUKCE

- Produkční prostředí má pro sebe dedikováno 13 serverů
- Typ BL685 – servery sa1x167 až sa1x179 – 4 x procesor AMD 2,6 GHz / 8 jader, min 256 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Produkčního Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - Nastavena redundance N+3
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
    - Pravidla: protože se jedná o „produkci", musíme mít nastavena pravidla pro rozdělení virtuálních serverů mezi fyzické. Tj. aplikace více serverová (například ESS, kde je více serverů mezi které se rozkládá zátěž) je nastavena tak, aby tato skupina serverů běžela pokuď možno na vícero fyzických serverech. Při výpadku jednoho nebo více fyzických serverů, je zaručeno, že aplikace stále poběží. (Pravidla jsou nastavena po čtyřech serverech)
- Tento cluster je nastaven, tak aby poskytoval maximální výpočetní výkon pro dané servery i v případě výpadku tří z daných serverů. Zároveň je nastaven tak, aby poskytoval vysokou dostupnost aplikací.

### 4.1.4 ESB_BACKEND

- ESB_Backend prostředí má pro sebe dedikovány 4 servery
  - Tyto čtyři servery jsou jak z KP1 tak z KP2 ( sa1x165, sa1x166, sa2x165, sa2x166 )
  - Toto netypické rozloženi serverů je dáno technologií MS, jedná se o tzv. geo-cluser
  - V tomto prostředí jsou tři pod organizační jednotky, které určují prioritu přidělování zdrojů:
    - Integrace
    - Test
    - Produkce
  - Toto nastavení zaručuje vždy prostředky pro produkci, pokud zbyde tak pro Test a v poslední řadě pro Integraci
- Typ BL685 – servery sa1x165, sa1x166, sa2x165, sa2x166 – 4 x procesor AMD 2,6 GHz / 8 jader, min 256 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Produkčního Clusteru:
  - Zapnuto On vSphere HA
    - Zapnuto Host Monitoring
    - Zapnuto Admission Control
    - Nastavena redundance není, jelikož se jedná o clusterové řešení
  - Zapnuto On vSphere DRS
    - Automation Level: Manual
- Tento cluster je nastaven tak, aby poskytoval maximální možnou funkcionalitu v rámci technického řešení.




demonstrace ESB_Backend

## 4.2 DATOVÉ CENTRUM KP2

- Má pod sebou čtyři organizační podsložky, tzv. „VMware Clustery" tyto clustery jsou:
    - Integrace
    - Test
    - Produkce

- Integrace, Test, Produkce mají stejné nastavení v lokalitě KP1 a v lokalitě KP2. Cluster ESB_Backend je speciální a nachází se v pouze v lokalitě KP1 i když je rozkročen přes obě lokality. Je to z důvodu technického řešení, v této organizační struktuře se nacházejí servery jak z integrace, testu, tak i z produkce a sdílejí mezi sebou zdroje.

### 4.2.1 INTEGRACE

- Integrační prostředí má pro sebe dedikované 4 servery
- Typ BL685 – servery sa2x157 až sa2x160 – 4 x procesor AMD 2,6 GHz / 8 jader, min 128 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Integračního Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - Nastavena redundance N+1
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
        - Power Management: Automatic (se střední hodnotou)

- Tento cluster je nastaven tak, aby poskytoval dostatek výpočetního výkonu pro dané servery i v případě výpadku jednoho z daných serverů. Zároveň je nastaven tak aby se choval ekonomicky a v případě nevyužitého výkonu převedl daný server do režimu spánku.

### 4.2.2 TEST

- Testovací prostředí má pro sebe dedikované 4 servery
- Typ BL685 – servery sa2x161 až sa2x164 – 4 x procesor AMD 2,6 GHz / 8 jader, min 128 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Testovacího Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - A nastavena redundance N+1
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
        - Power Management: Automatic (se střední hodnotou)

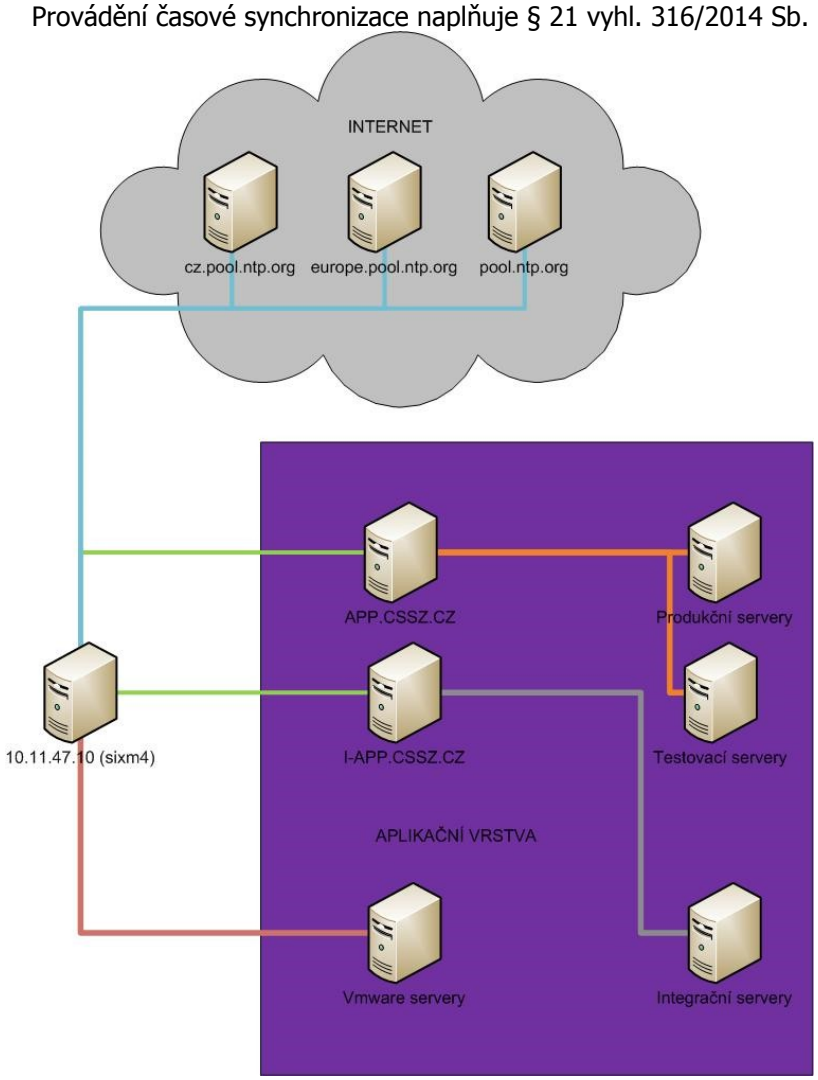
- Tento cluster je nastaven, tak aby poskytoval dostatek výpočetního výkonu pro dané servery i v případě výpadku jednoho z daných serverů. Zároveň je nastaven tak aby se choval ekonomicky a v případě nevyužitého výkonu převedl daný server do režimu spánku.

### 4.2.3 PRODUKCE

- Produkční prostředí má pro sebe dedikováno 13 serverů
- Typ BL685 – servery sa2x167 až sa2x179 – 4 x procesor AMD 2,6 GHz / 8 jader, min 256 GB RAM, 2x 72 GB HD / HDD se může lišit dle dodávky /
- Nastavení Produkčního Clusteru:
    - Zapnuto On vSphere HA
        - Zapnuto Host Monitoring
        - Zapnuto Admission Control
        - A nastavena redundance N+3
    - Zapnuto On vSphere DRS
        - Automation Level: Fully automated (se střední hodnotou)
    - Pravidla: protože se jedná o „produkci", musíme mít nastavena pravidla pro rozdělení virtuálních serverů mezi fyzické. Tj. aplikace více serverová (například ESS, kde je více serverů mezi které se rozkládá zátěž) je nastavena tak, aby tato skupina serverů běžela poluď možno na vícero fyzických serverech. Při výpadku jednoho nebo více fyzických serverů, je zaručeno, že aplikace stále poběží.
- Tento cluster je nastaven, tak aby poskytoval maximální výpočetní výkon pro dané servery i v případě výpadku tří z daných serverů. Zároveň je nastaven tak aby poskytoval vysokou dostupnost aplikací.

# 5. ČASOVÁ SYNCHRONIZACE

- Časová synchronizace se provátí skrz tzv. časové servery (time servery). Je bezpodmínečně nutné mít veškeré aplikační servery komunikující mezi sebou časově synchronizovány (stejný čas). Pokud by servery neměly stejný čas, nefungovala by komunikace mezi servery a ani s DB !!!
- V aplikační vrstvě jsou dva časové servery:
  - Integrační
  - Produkční + Testovací
- Tyto servery jsou řadiče domén (app.cssz.cz a i-app.cssz.cz /jedná se o tzv. PDC emulátory/).
- Všechny servery ať, virtuální nebo fyzické s OS Windows a Linux, se synchronizují od nich. (dle příslušnosti prostředí).
- Servery, se v aplikační vrstvě provozu VMware synchronizují od zdroje v ČSSZ (sixl1) tj. stejný časový server od kterého se synchronizují domény app.cssz.cz a i-app.cssz.cz
- Provádění časové synchronizace naplňuje § 21 vyhl. 316/2014 Sb.

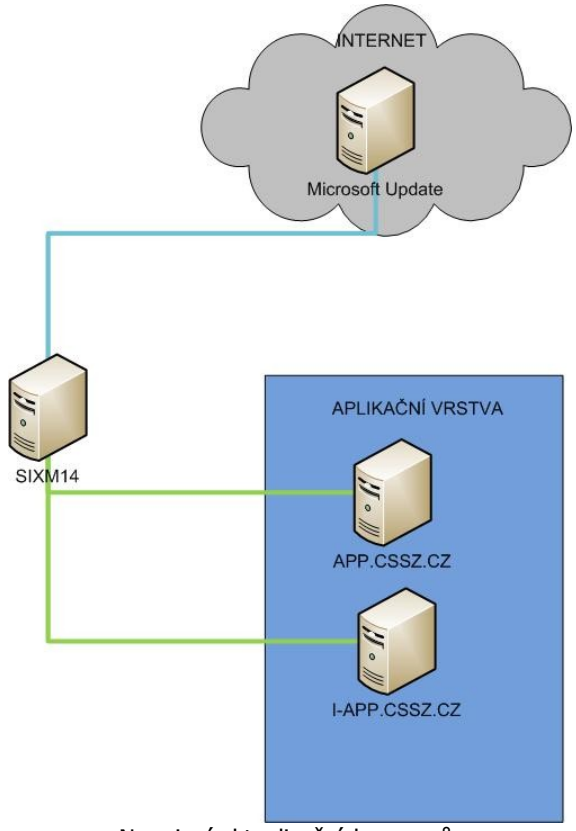


# 6. PRINCIP AKTUALIZACÍ V APLIKAČNÍ VSTVĚ

- V každé příslušné kapitole je vysvětleno jakým způsobem se bude provádět aktualizace serverů. Zde bude standardizován aktualizační proces a nastíněno parciální fungování aktualizačního procesu.

## 6.1 WSUS

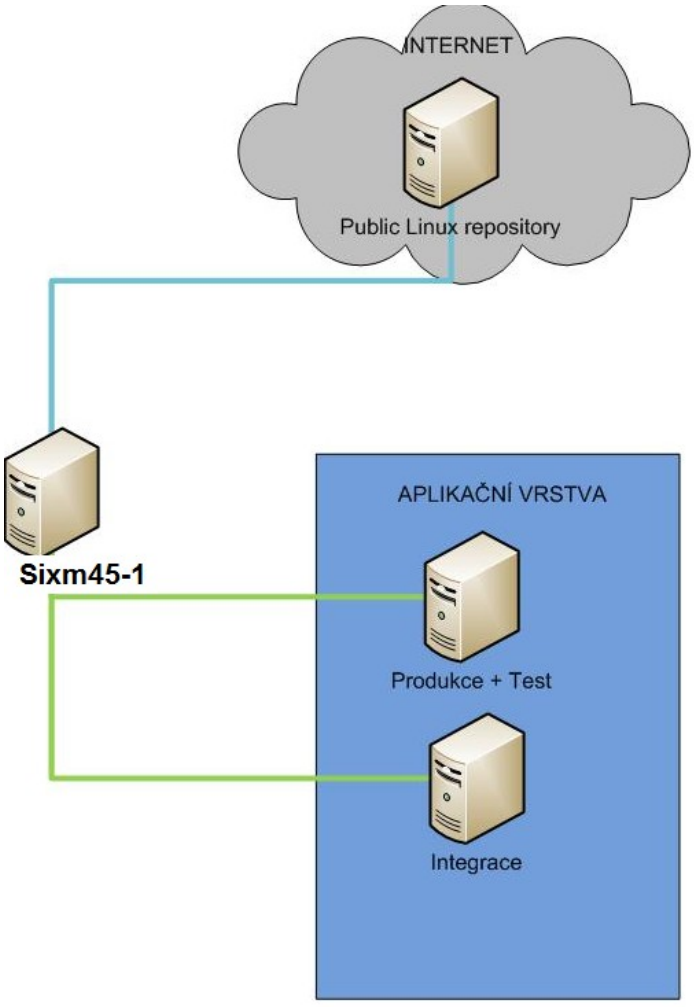
- Aktualizace pomocí WSUS jsou již zmíněny v příslušných kapitolách standardu. Jedná se o aktualizační server pro produkty rodiny Microsoft.
- Aktualizaci běžících serverů provádí jednotliví správci aplikačních serverů.
- Aktualizace jsou nabízeny automaticky.
- Individuální nastavení aktualizací je možné po dohodě s odd. 524
- Aktualizační proces je řízen příslušnou GPO v AD pro danou aplikační farmu
- Řazení serverů do aktualizačních skupin je dáno GPO (po aplikačních farmách, vždy servery jedné aplikační farmy mají dostupné stejné aktualizace)
- WSUS server je nainstalován na AD serveru, vždy v lokalitě KP1
- Stahují se následující aktualizace
    - Critical updates
    - Definition updates
    - Security updates
- WSUS server se pokouší stáhnout aktualizace každý den v 3:00




Napojení aktualizačních serverů.

## 6.2 LINUX REPOSITORY

- Aktualizace pomocí Linux repository jsou již zmíněny v příslušných kapitolách standardu. Jedná se o aktualizační server pro Linux v našem případě pro Linux CENTOS.
- Aktualizaci běžících serverů provádí jednotliví správci aplikačních serverů.
- Aktualizace jsou dostupné automaticky.
- Individuální nastavení aktualizací se provádí na daném aplikačním serveru
- Aktualizační proces je řízen správcem aplikace nebo skriptem
- Linux repository server je nainstalován v síti kde funguje WSUS server, vždy v lokalitě KP1
- Stahují se veškeré aktualizace jednotlivých programu i celého OS
- Linux repository server se pokouší stáhnout aktualizace každý den v 3:00
- U linuxové distribuce CENTOS se stahují RPM balícky (balíčkovací systém původně pro RedHat)
- Aktualizace systémů Linux CENTOS se provádí příkazem „yum"




Napojení aktualizačních serverů

## 6.3 VMWARE

- VMware se aktualizuje manuálně, tj. stažení aktualizací provádí odd. 524.
- Příprava aktualizačního procesu provádí odd. 524 s dodavatelem.
- Většinou aktualizace nevyžadují přerušení provozu, proto se mohou provádět i za provozu.
- Aktualizace se provádějí zpravidla 2-3 měsíce po uvedení, pokud neopravují kritickou funkční nebo bezpečnostní chybu, pak se instalují ihned!

# 7. SNMP

- **SNMP** je asynchronní transakčně orientovaný protokol pracující nad UDP na modelu **KLIENT/SERVER.** Obdobou je například **WMI** od firmy ***Microsoft***. Podporu **SNMP** má velká řada zařízení, například aktivní síťové prvky, počítačová čidla, tiskárny, přístupové body nebo pomocí softwaru a ovladačů ji mohou získat osobní počítače a servery. Hodnoty můžeme získávat v pravidelném intervalu a ty pak jednoduše ukládat do databáze spolu s časem a následně vykreslit do grafu. Přehledně tak můžeme zobrazit třeba vytížení procesoru, průběh teploty nebo datový tok na portu přepínače.

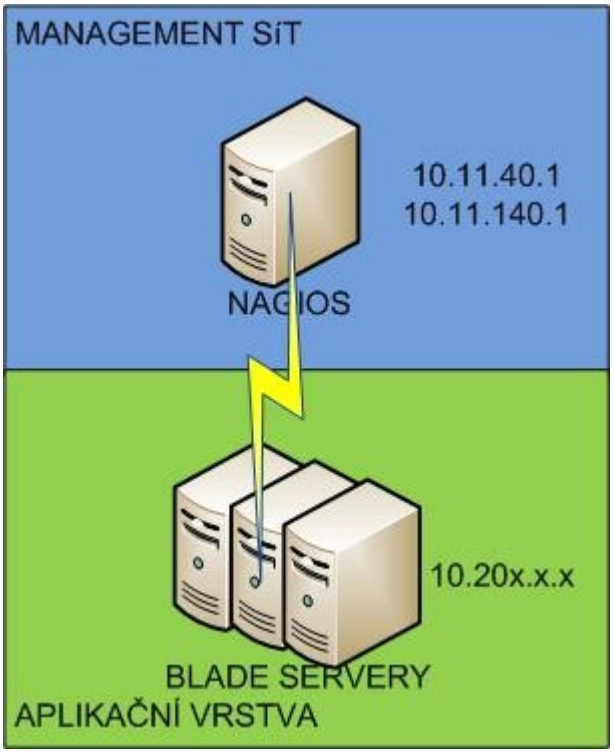
- SNMP manager SERVER je program, který běží na síťové stanici. Může to být jednoduchý prohlížeč SNMP, ale také složitý NMS (Network Management System). Funkce spočívá v dotazování jednotlivých SNMP agentů pomocí SNMP operací. Smyslem je získat všechny potřebné informace o daném zařízení, které agent reprezentuje. SNMP manažer poskytuje většinou grafické rozhraní, které umožňuje prezentaci získaných dat, sledování síťových alarmů a archivaci dat (např. k analýze časového vývoje).

- SNMP agent SERVER je malý program, běžící na síťovém zařízení, který jej reprezentuje a odpovídá na dotazy SNMP manažera. Agent proto neustále monitoruje a sbírá informace o všech dostupných funkcích a stavech daného zařízení. Tyto základní a přídavné informace se spolu nazývají *MIB (Management Information Base)*. MIB je datová hierarchická stromová struktura, která odpovídá danému konkrétnímu zařízení.

  Informace mohou být také vyslány agentem bez vyžádání manažerem. Jestliže agent detekuje jisté podmínky(jako např. výpadek proudu, větráku, překročení mezních údajů, objevení nového zařízení), vyšle tuto informaci, zvanou trap, sám bez vyžádání. To je důležité pro zajištění okamžité informovanosti např. o vážnějších problémech, protože tzv. polling aktivita manažera - procedura vyžádání informací - je nastavitelná v jistých intervalech.

  Pro většinu informací není nutné kontinuální monitorování (neprovádí se také z důvodu zbytečné zátěže sítě), a tak kombinace polling aktivity managera a trap aktivity agenta zajišťují potřebnou efektivitu.

  Teprve když manager přijme varovný trap od zařízení, může se více zaměřit na toto problémové místo - tzv. trap directed polling. Protože traps jsou ale nepotvrzované pakety a doručení není spolehlivé, nelze se spolehnout na to, že nedostáváme-li žádné traps, všechno na síti je v pořádku!




Pricnip pro APL vrstvu

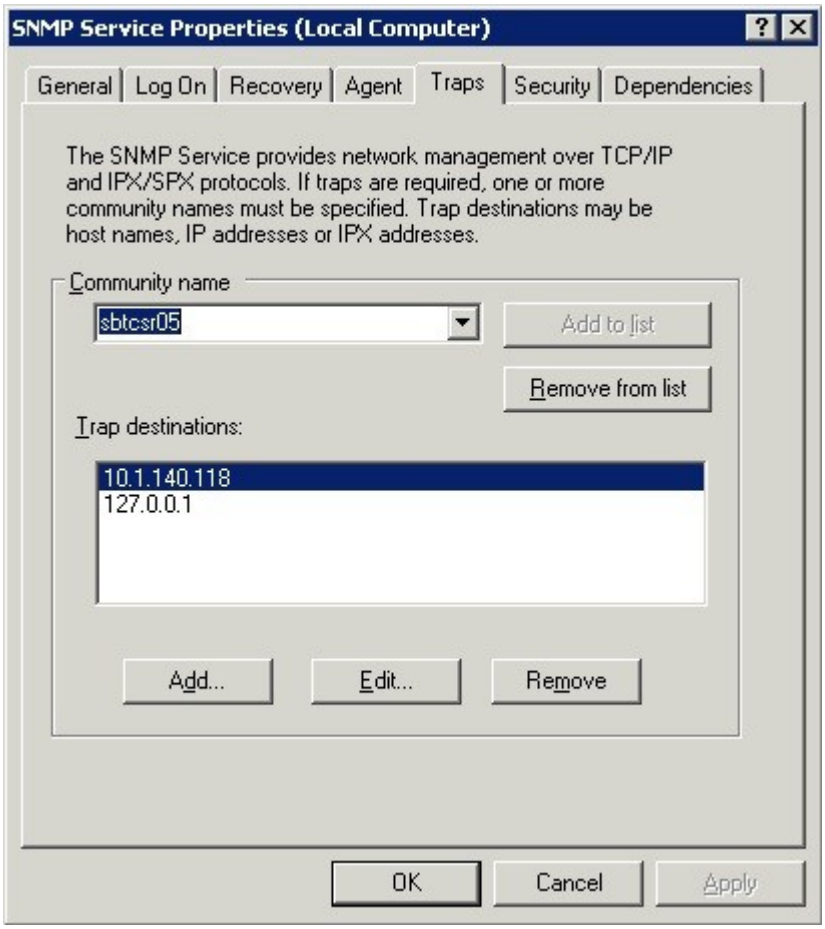
Aplikační vrstva:

Dnes se na aplikační vrstvě používá SNMPv2 a nachází v APPV několik SNMP komunit:

| SNMP Komunita | Popis |
|---|---|
| ad82d01d-de47-4555-94db-3386970f7f5e | Generována při použití MS produktů. |
| anf413 | Toto je komunita pro ATOS, který má svůj Nagios. |
| PUB_APP_CSSZ | |
| PUB_NAG_CSSZ | Toto je komunita pro MONITORING ČSSZ Nagios. |
| PUB_ORG_CSSZ | |
| Public | Defaultní komunita |
| sbtcsr05 | Tato komunita je pro READ a je primárně určena pro SIM |
| sbtcsw05 | Tato komunita je pro WRITE a je primárně určena pro SIM. Asi se nevyužívá. |

TRAP:

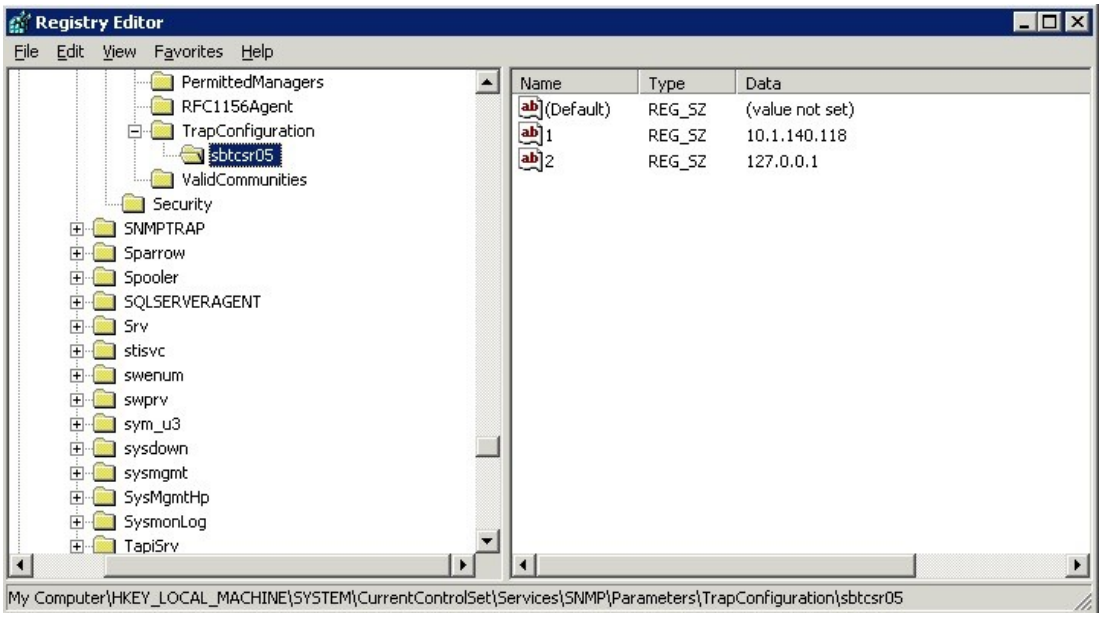
Pro ilustraci, ve Službách Windows se nachází služba SNMP, v jejích vlastnostech se dá nastavit SNMP trap:




Jedná se o vlastnost, kdy na sledovaných prostředcích dojde k problému a tato služba sama zkontaktuje monitorovací server v našem případě NAGIOS.

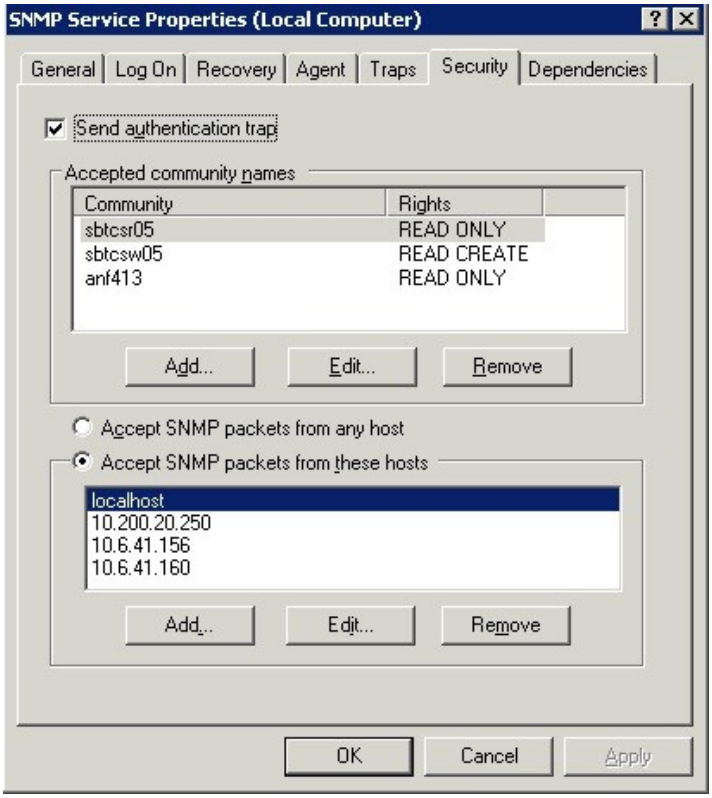
Úprava v registrech je na v cestě:

*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\TrapConfiguration*



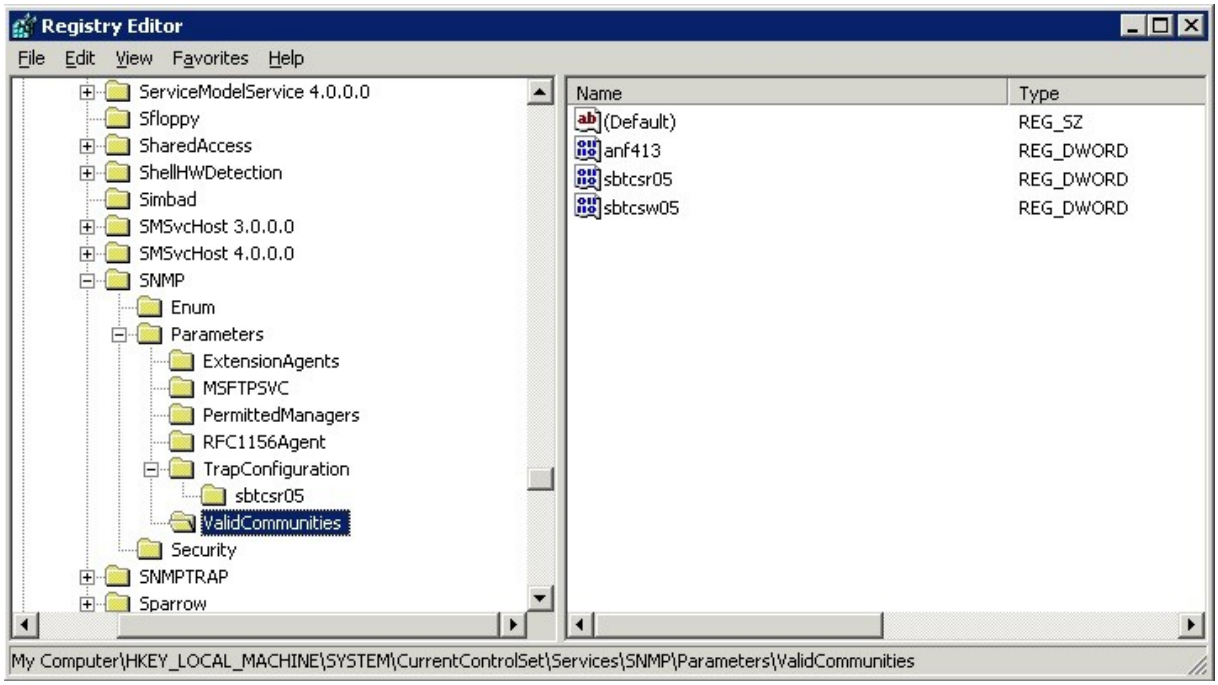

Jak je vidět v registrech Windows pod *„TrapConfiguration"* je složka která koresponduje s trap komunitou, ve které jsou hodnoty korespondující s cílem zasílání.

Community:

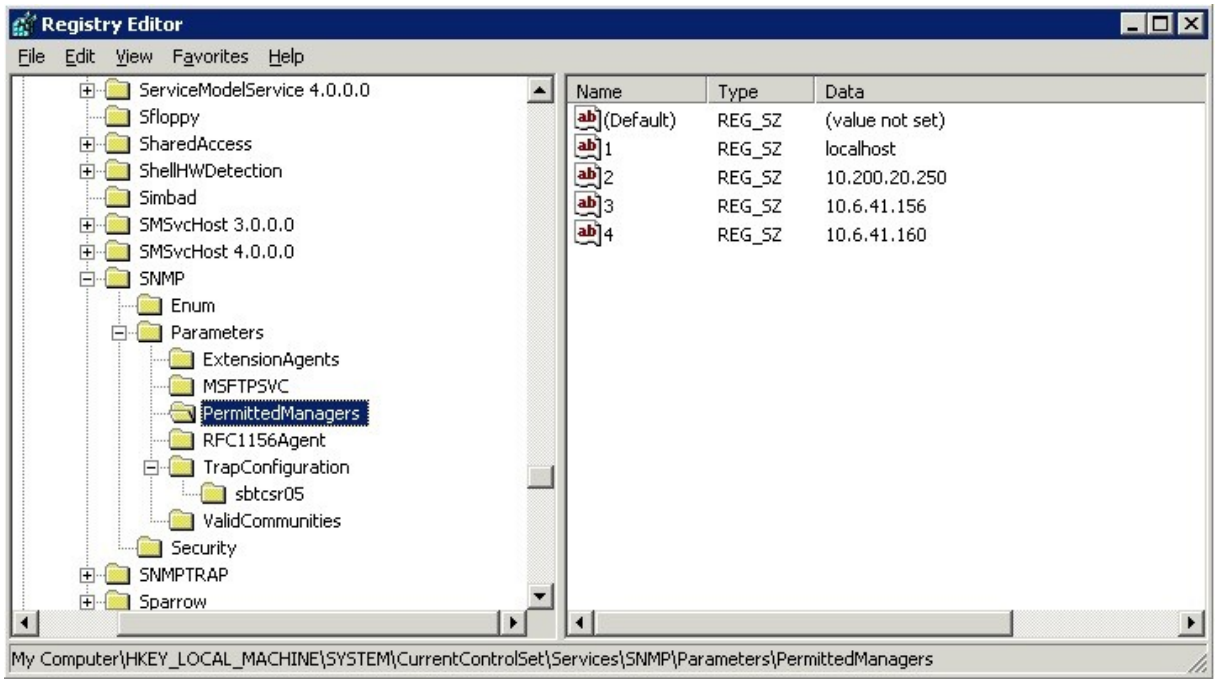



Nastavení Community pro SNMP nad službou SNMP Windows.

V horní části community kterou se autentifikují klienti SNMP a v dolní části z jakých IP adres mohou přistupovat.




Obrázek kde se nacházejí v registrech Windows povolené community.




Obrázek kde se nacházejí v registrech Windows povolené IP community.

# 8. TVORBA HESEL, ÚČTŮ A JEJICH PRAVIDLA

- Tvorba uživatelských účtů v aplikační vrstvě se řídí jednoduchými pravidly:

1) Volba domény / prostředí, tedy zda app či i-app
2) První tři písmena z příjmení a první tři písmena z jména, může při této kombinaci dojít i ke shodě. Tato shoda se řeší tak, že šesté písmeno nahradíme číslem.
3) Přípona dle typu účtu:
    - „-a" Administratorský účet
    - „-d" Doménový správce
    - „-o" Operátorský účet

- Uživatelské účty mají pevnou délku, pro integrační prostředí je délka 12 znaků a pro produkční/testovací prostředí je délka 11 znaků. Pár příkladů pro uživatele Jan Strnad:

1) appstrjan-d - Doménový administrátor v doméně app.cssz.cz
2) appstrjan-a - Administrátor dané aplikace v doméně app.cssz.cz
3) appstrjan-o - Operátor dané aplikace v doméně app.cssz.cz
4) iappstrjan-d - Doménový administrátor v doméně i-app.cssz.cz
5) iappstrjan-a - Administrátor dané aplikace v doméně i-app.cssz.cz
6) iappstrjan-o - Operátor dané aplikace v doméně i-app.cssz.cz

- dalším typem doménového účtu jsou tzv. servisní účty. Servisní účty jsou pomocné účty dané aplikace, v doméně, jejich konvence jsou následovné:

1) učet začíná „srv" nebo po novu „tu"
2) pak následuje „aplikace"
3) poslední součást jména je účel účtu

    - Příklad účtu: „srv_ess_rep" / „tu_ess_rep" tento účet například je určen k replikaci.

- Lokální účty na aplikačních serverech zařazených do domény nejsou povoleny !

- Doménová politika přikazuje minimální délku a složení hesla, tato pravidla platí i pro nedoménové servery.

- Heslo má minimální délku 15 znaků, musí obsahovat velká, malá písmena, číslice a speciální znak například: „#,@ nebo > atd.."

- Minimální doba pro povinnou výměnu hesla je 90 dnů.

- Není možné vícekrát měnit heslo za časové období 24 hodin.

# 9. SÍŤOVÁ INFRASTRUKTURA APLIKAČNÍ VRSTVY

- Aplikační servery jsou děleny do VLAN.
- Každá aplikace má svoji VLAN.
- Jsou v zásadě dva druhy aplikačních VLAN
  - balancovaná
    - Tento druh VLAN se balancuje dvěma metodami
      - Round-robin
      - Least connections
  - Nebalancovaná
    - Zde jsou v zásadě dva druhy VLAN
      - Klasická aplikační VLAN bez balancingu, kde není třeba rozklad zátěže (např. dávkové ulohy)
      - BTS VLAN, která je rozložena přes dvě lokality, kvůli MS clusteru.
- Rozklad zátěže probíhá na základě dvou parametrů na sobě závislých
  - Odpovědi na „ping", tedy zda server žije či ne
  - Odpovědi na keep a live URL/ Application status (více kapitola 10)
- Systém „provisioning" umožnuje jednotlivé servery vyřadit z balancingu, např. v případě náhlého problému. Stav Active /probíhá balancing/ nebo stav /Install balancing pro daný server neprobíhá/, provádí odd. 524.
- Samotný balancing probíhá na tzv. „virtuální IP adresu", tato IP adresa za sebou schovává všechny balancované servery dané aplikace.
- Aplikační vrstva se skládá z dvou geograficky oddělených datových center
  - KP_1 (Křížová 6a)
  - KP_2 (Trojská 13)
- Každé data centrum má vlastní rozsah IP adres a DNS záznamy
  - Server s DNS názvem SA1X001 je z KP_1 (jedná se o první server v KP_1 což reperezentuje „001", lokalitu reprezentuje předpona „SA1X")
  - Server s DNS názvem VA1X131p01 je z KP_1 (jedná se o první virtuální server „p01" v VLAN „131" v KP_1 „VA1X". IP adresa takového to serveru bude 10.200.131.180
    - Řetězec „p01" identifikuje prostředí „p" což je produkce, tedy IP adresa pro produkci v KP_1 (KP_1 identifikuje řetězec „VA1") začíná 10.200.X.Y. Třetí bajt IP adresy je 131(aplikace ESS), který plyne z názvu serveru, tedy 10.200.131.Y. Poslední bajt IP adresy je 180 což určuje řetězec „01".Pokud by byl na konci názvu řetězec „02" poslední bajt by byl 181 atd.
  - Server s DNS názvem SA2X001 je z KP_2 (jedná se o první server v KP_2 což reprezentuje „001", lokalitu reprezentuje předpona „SA2X")

- Server s DNS názvem VA2X131p01 je z KP_2 (jedná se o první virtuální server „p01" v VLAN „131" v KP_2 „VA2X". IP adresa takového to serveru bude 10.201.131.180

    - Řetězec „p01" identifikuje prostředí „p" což je produkce, tedy IP adresa pro produkci v KP_2 (KP_2 identifikuje řetězec „VA2") začíná 10.201.X.Y. Třetí bajt IP adresy je 131(aplikace ESS), který plyne z názvu serveru, tedy 10.201.131.Y. Poslední bajt IP adresy je 180 což určuje řetězec „01".Pokud by byl na konci názvu řetězec „02" poslední bajt by byl 181 atd.

- IP adresy a prostředí:

    - 10.200.X.Y – Produkce KP_1
    - 10.201.X.Y – Produkce KP_2
    - 10.202.X.Y – Test KP_1
    - 10.203.X.Y – Test KP_2
    - 10.204.X.Y – Integrace KP_1
    - 10.205.X.Y – Integrace KP_2

- Samozřejmě existují výjimky jak v IP adresách, tak v názvech, nejedná se o klasické servery aplikační vrstvy, nebo klasické aplikace.

- Vytváření nových VLAN provádí pro ČSSZ dodavatel na základě písemného požadavku. Správu sítového prostředí aplikační vrstvy provádí tentýž dodavatel.

- Aplikace mezi sebou komunikují na portu 80, s jakými aplikacemi muže daná aplikace komunikovat a jakým stylem se musí specifikovat! Není povoleno standardně.

# 10. KEEP A LIVE URL / APPLICATION STATUS

- Jedná se o funkcionalitu aplikace v aplikační vrstvě, která indikuje, zda je aplikace funkční a tedy připravena komunikovat.

- Primárně je určen k ověření dostupnosti aplikace na aplikačním serveru a následném nasměrování zátěže (při rozkládání zátěže pomocí aktivních prvků si prvky / systém provisioning kontrolují Keep a live URL / Application Status pokud je dostupný, pošlou komunikaci)

- Momentálně většina aplikací Keep a live URL / Application Status respektuje. Nicméně práce s touto důležitou komponentou v aplikační vrstvě by měla být mnohem více interaktivní.

- Dnes některé aplikace mají na svém serveru rozběhnutý nějaký webový server, který má na sobě vystavenou neinteraktivní stránku indikující Keep a live URL / Application Status například „index.htm". Tedy tento stav neumožnuje indikovat nefunkčnost aplikace a tedy i při nefunkčnosti aplikace je na ni nadále provoz.

- Obecná pravidla pro sestavení příslušného URL:

**http://SERVER/ApplicationStatus/wsApplicationStatus.asmx**

  - Červená barva značí neměnný řetězec
  - Hnědá barva značí DNS záznam serveru
  - Žlutá barva značí typ použité technologie (ASP,PHP,JSP, …)

- Standard fungování Keep a live URL / Application Status:

- Funkcionalita nadále musí být zachována, Keep a live URL / Application Status musí být součástí aplikace a zahrnuje dva základní okruhy:

1) Obecné zjištění funkcionality (perioda 3 min):
   a) Zjištění dostupnosti sítové konektivity, příslušných DNS záznamu a DB
   b) Zjištění dostupnosti klíčových systémových služeb a komponent
   c) Zjištění dostupnosti všech potřebných zdrojů z pohledu systému

2) Aplikační zjištění funkcionality:
   a) Kontrola přístupnosti DB a tabulek
   b) Kontrola funkcionality klíčových aplikačních služeb, komponent
   c) Spuštění testovacích dat pro ověření konzistence aplikace na daném serveru

# 11. ZÁVĚR

- Tento dokument standardizuje principy a fungování aplikační vrstvy a slouží jako pomůcka pro dodavatele ČSSZ. Jelikož naše prostředí je poměrně robustní a komplikované, měl by tento dokument dopomoci k bezproblémové implementaci nových aplikací a technologií.

- Dokument se snaží jít cestou nejmenšího odporu. Klade na aplikace a prostředí nároky, které se snaží zabránit nevhodnému mixování technologií. Také se snaží více otevřít levnějšímu open-source řešení, minimálně z pohledu OS.

- Povolené kombinace technologií:

  1) **Microsoft Windows + Net. FrameWork**
  2) **Linux + Java**

- Tento dokument nepopisuje způsob zálohování a obnovy aplikačních serverů. Bude řešeno v další verzi standardu.
- Aktualizace firmware jednotlivých blade komponent provádí odd. 524 ve spolupráci s dodavatelem jednou za ¼ roku.
- Servisní okna pro aplikační servery, tedy pro aplikace a jejich instalace jsou:
  - Každý čtvrtek po 16:00
  - Náhradní termín je následující Úterý po 16:00
- Schematické zobrazení aplikační vrstvy z pohledu komunikace: