

Název projektu:	<b>System automatizované kontroly a detekce změn bezpečnostního nastavení informačních systémů založený na specifikaci bezpečnostní politiky podle standardu BS7799</b>
Číslo projektu:	<b>1F43D/007/030</b>

Název zprávy:	<b>Závěrečná zpráva projektu</b>
Název části:	<b>Uživatelská příručka</b>
Období:	<b>1.1.2005-31.12.2005</b>

Poskytovatel:	<b>Ministerstvo dopravy ČR</b>
Příjemce:	<b>WAK System, spol. s r.o.</b>
Adresa příjemce	<b>Petržilkova 2564/21, 158 00 Praha 5 - Stodůlky</b>

Odpovědný řešitel:	<b>Ing. Radan Kasal</b>
Spoluřešitelé:	<b>Ing. Luděk Benda</b>
	<b>Ing. Tomáš Nagy</b>
	<b>Ing. Petr Půlpán</b>
	<b>Radek Valeš</b>
	<b>RNDr. Miroslav Wasserbauer</b>
	<b>Ing. Vítězslav Života</b>
	<b>Tibor Stiliz</b>

Datum vydání:	<b>31.1.2006</b>
---------------	------------------



# Úvod

Uživatelská příručka ukazuje na příkladech možnosti nastavení jednotlivých položek konfiguračních souborů systému. Součástí je i popis výstupů.

## 1. Popis

Systém je koncipován jako aplikace s rozhraním ve formě univerzálních souborů formátu XML. Možnosti dalšího rozšíření a obohacení systému dalšími formami vstupu a výstupu jsou velké a relativně jednoduché.

Následující příklady popisují výstupní soubory a možná nastavení serverového konfiguračního souboru `SysKoServer\App.config` a klientského konfiguračního souboru `SysKoConsole\App.config`. Tučným písmem je popsán příslušný komentář.

## 2. Konfigurační soubor SysKoServer

V následující kapitole je uvedeno možné nastavení serverového konfiguračního souboru.

### 2.1 Příklad nastavení

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="sysko">
```

```
<section name="appConnectionString"  
type="Wak.Wnt.Db.DbConnectionStringConfigurationSectionHandler, Wak.Wnt.Db" />
```

```
<section name="notification"  
type="Wak.SysKo.As.Server.NotificationConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="checkSystem"  
type="Wak.SysKo.As.Server.CheckSystemConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="accessRights"  
type="Wak.SysKo.As.Server.AccessRightsConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
<section name="checkQuery"  
type="Wak.SysKo.As.Server.CheckQueryConfigurationSectionHandler,  
Wak.Sysko.As.Server" />
```

```
</sectionGroup>
```

```
<sectionGroup name="wak.wnt.remoting">
```

```
<section name="appConnectionString"  
type="Wak.Wnt.Db.DbConnectionStringConfigurationSectionHandler, Wak.Wnt.Db" />
```

```
<section name="wellknown"  
type="Wak.Wnt.Tools.Remoting.RemotingConfigurationSectionHandler, Wak.Wnt.Tools" />
```

```
<section name="channel"  
type="Wak.Wnt.Tools.Remoting.RemotingConfigurationSectionHandler, Wak.Wnt.Tools" />
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <sysko> ta je určena k nastavení uživatelských parametrů systému.**

```
<sysko>
```

```
<appConnectionString database="sysko" server="server1" uid="sa" pwd="sa" />
```

**Specifikuje databázi pojmenovanou “sysko”, s oprávněním pro přístup uživatelského jména a hesla “sa”, umístěnou na serveru pojmenovaném “server1”.**

```
<notification >
```

```
<group id="fileReport" smtpserver="smtpserver" mailfrom="sysko@test.cz"
directory="c:\program files\SysKo\output">
```

**Atributem id je definována jedna skupina s identifikátorem “fileReport”. Atribut smtpserver definuje SMTP server pojmenován “smtpserver”. Výstupy budou ukládány do adresáře “c:\program files\SysKo\output”, definovaného atributem directory.**

```
<target proto="file" xslt="" css="@ @ACTION@ @.css" name="@ @DATE:yyyy-MM-
ddTHH-mm-ss@ @ _ @ACTION@ @.xml" />
```

**Atributem proto je nastaven způsob notifikace pomocí výstupních souborů. Atribut xslt je nastaven na prázdnou hodnotu. Takto není na výstupní soubor použita XSL transformace a soubor zůstane ve formátu XML. Pokud bychom chtěli použít XSL transformaci, definovali bychom hodnotu atributu xslt např. takto: "html\_@ @ACTION@ @.xslt". Atribut css není při prázdném atributu xslt podstatný. V atributu name je použito makro @ @ACTION@ @ a @ @DATE@ @, makro @ @ACTION@ @ bude nahrazeno hodnotou atributu odkazujícího elementu <notify>. Hodnotou makra @ @DATE:yyyy-MM-ddTHH-mm-ss@ @ bude datum notifikace.**

```
</group>
```

```
<notify id="stationList" action="stationList" sendTo="fileReport" interval="20" />
```

**Atributem id je tato notifikace identifikována jako "stationList". Typ notifikace je nastaven atributem action na "stationList". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Periodicita notifikace je 20 minut.**

```
<notify id="eventLog" action="eventLog" sendTo="fileReport" stationID="192.168.% "
interval="20" />
```

**Atributem id je tato notifikace identifikována jako "eventLog ". Typ notifikace je nastaven atributem action na "eventLog". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.**

```
<notify id="scanList" action="scanList" sendTo="fileReport" stationID="192.168.%"  
interval="20" />
```

**Atributem id je tato notifikace identifikována jako "scanList". Typ notifikace je nastaven atributem action na "scanList". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.**

```
<notify id="scanDiff" action="scanDiff" sendTo="fileReport" stationID="192.168.%"  
interval="20" />
```

**Atributem id je tato notifikace identifikována jako "scanDiff". Typ notifikace je nastaven atributem action na "scanDiff". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Předmětem notifikace jsou stanice jejichž IP adresa začíná na "192.168". Periodicita notifikace je 20 minut.**

```
<notify id="checkSystem" action="checkSystem" sendTo="fileReport" interval="20"/>
```

**Atributem id je tato notifikace identifikována jako "checkSystem". Typ notifikace je nastaven atributem action na "checkSystem". Cíl notifikace je element <group> s atributem id jehož hodnotou je "fileReport". Periodicita notifikace je 20 minut.**

```
</notification>
```

```
<accessRights>
```

```
<stationGroup id="localhost">
```

```
  <station stationID="^" />
```

```
</stationGroup>
```

**Je definována skupina stanic, která je atributem id identifikována jako localhost.**

```
<process typeID="Wak.SysKo.As.Server.Scan_tr">
```

```
  <allowGroup groupID="localhost" />
```

```
</process>
```

**K procesu "Wak.SysKo.As.Server.Scan\_tr" má povolena přístup skupina stanic identifikována jako "localhost". V následujících elementech <process> se skupině "localhost" povoluje přístup k dalším procesům.**

```
<process typeID="Wak.SysKo.As.Server.EventLog_tr">
```

```
  <allowGroup groupID="localhost" />
```

```
</process>
```

```
<process typeID="Wak.SysKo.As.Server.Report_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.BS7799_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.CheckSystem_tr">
  <allowGroup groupID="localhost" />
</process>
<process typeID="Wak.SysKo.As.Server.CheckQuery_tr">
  <allowGroup groupID="localhost" />
</process>
</accessRights>
</sysko>
<wak.wnt.remoting>
  <wellknown mode="Singleton" name="SysKoManager"
  type="Wak.SysKo.As.Server.SysKoManager" />
  <channel ref="tcp" port="10082">
Komunikace se SysKoManagerem bude probíhat přes protokol tcp na portu 10082.
  </channel>
</wak.wnt.remoting>
</configuration>
```

### 3. Nastavení kontroly BS7779

Pro nastavení vzoru bezpečnostní politiky slouží grafické rozhraní. Aktuální vzor je pak v případě testů porovnáván se skutečnou politikou sledovaného OS.

Název	Kapitola BS7799	Typ hodnot	Dopor. hodnota	Akt. hodnota	Operátor
<input type="checkbox"/> Vynutit použití historie hesel	9.5.4	value	0		=
<input type="checkbox"/> Maximální stáří hesla	9.5.4	value	120		<=
<input checked="" type="checkbox"/> Minimální stáří hesla	9.5.4	value	0	10	=
<input checked="" type="checkbox"/> Minimální délka hesla	9.5.4	value	6	6	>=
<input type="checkbox"/> Složitost hesla	9.5.4	bool	A		=
<input checked="" type="checkbox"/> Způsob uchování hesla	9.5.4	bool	N	N	>=
<input type="checkbox"/> Doba uzamčení účtu	9.3.2	value	30		<=
<input type="checkbox"/> Prahová hodnota pro uzamknutí účtu	9.5.2	value	3		<=
<input type="checkbox"/> Výmulování čítače pro zamknutí účtu	9.5.2	value	30		<=
<input type="checkbox"/> Vynutit omezení přihlášení uživatele	9.6.1	bool	A		=
<input type="checkbox"/> Maximální doba života lístku služby	9.5.7	value	600		=
<input type="checkbox"/> Maximální doba života lístku uživatele	9.5.7	value	10		=
<input type="checkbox"/> Maximální doba života pro obnovení lístku uživatele	9.5.7	value	7		=
<input type="checkbox"/> Maximální tolerance synchronizace hodin počítače	9.7.3	value	5		=
<input type="checkbox"/> Auditovat události přihlášení k účtu	9.7.1	value	F		=

Obr. 1 Nastavení bezpečnostní politiky

Nastavení bezpečnostní politiky respektuje doporučení normy BS 7799. Popis jednotlivých sloupců:

- zaškrtnutý řádek ukazuje, že pro daný bezpečnostní parametr je nastavena vzorová hodnota
- název obsahuje přesný název bezpečnostního parametru podle používaného OS
- kapitola BS 7799 odkazuje na příslušnou část normy BS 7799
- typ hodnoty se vztahuje k hodnotě bezpečnostního parametru
- dopor. hodnota obsahuje optimální hodnotu podle BS 7799
- akt. hodnotu je možné přepsat, a tak nastavit vlastní vzor bezpečnostní politiky
- operátor se vztahuje k porovnání aktuální hodnoty bezpečnostního parametru a skutečné hodnoty parametru aktuální bezpečnostní politiky OS

Ovládací prvky:

**Seznam definovaných bezpečnostních politik** – uvedeny názvy, ze kterých je možné si vybrat. Při zadání nové vlastní politiky stačí do boxu zapsat vlastní název.

**Tlačítko Uložit** – uloží aktuálně zpracovávanou bezpečnostní politiku.

**Tlačítko Vrátit změny** – načte z databáze původní politiku před změnami v případě chybné definice.

**Tlačítko Smazat** – smaže aktuálně zpracovávanou bezpečnostní politiku.

## 4. Sledování událostí

### 4.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.**

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.**

```
<eventLog>
```

```
<events id="evttest">
```

**Identifikuje test, který sleduje události jako "evttest".**

```
<log name="system|application" source="SysKoTest" />
```

**Hodnota "system|application" atributu name elementu <log> specifikuje událost ze zdroje identifikovaného jménem "SysKoTest" ze systémového, nebo aplikačního logu.**

```
</events>
```

```
</eventLog>
```

```
</SysKo>
```

```
</configuration>
```

## 4.2 Příklad výstupního souboru

```
<EventLog xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<event>
```

**Element <event> popisuje jednu událost.**

```
<stationID>192.168.168.15</stationID>
```

**192.168.168.15 je IP adresa stanice na níž došlo k události.**

```
<logName>application</logName>
```

**Druh události.**

```
<machineName> STANICE </machineName>
```

**Jméno stanice.**

```
<eventDate>2006-01-30T17:39:56.0000000+01:00</eventDate>
```

**Datum události.**

```
<eventID>0</eventID>
```

**ID události.**

```
<eventType>Information</eventType>
```

**Typ události.**

```
<eventSource>SysKoTest</eventSource>
```

**Zdroj události.**

<eventDescription>SysKo test service Start.</eventDescription>

**Popis události.**

</event>

</EventLog>

## 5. Sledování souborů

### 5.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.**

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.**

```
<scanner>
```

```
<scan id="scantest">
```

```
<fileSystem name="c:\Program files\SysKo\test" recursive="0" />
```

```
</scan>
```

**Identifikuje scan jako "scantest". Sledovaným adresářem je "c:\Program files\SysKo\test". Prohledávání podadresářů je atributem recursive vypnuto.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

## 5.2 Příklad výstupního souboru

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

**IP adresa sledované stanice.**

```
</station>
```

```
<scan1>
```

**Scan před změnou.**

```
<scanID>scantest</scanID>
```

**ID scanu.**

```
<scanDate>2006-01-30T18:23:11.5600000+01:00</scanDate>
```

**Datum scanu.**

```
</scan1>
```

```
<scan2>
```

**Scan po změně.**

```
<scanID>scantest</scanID>
```

**ID scanu.**

```
<scanDate>2006-01-30T18:23:27.3770000+01:00</scanDate>
```

**Datum scanu.**

```
</scan2>
```

```
<objectOS>
```

```
<name>c:\Program files\SysKo\test\SysKoTestFile.txt</name>
```

**Celá cesta k souboru.**

```
<type>file</type>
```

**Typ.**

<Values>

<name>fileLastWriteTime</name>

**Čas poslední modifikace souboru.**

<diffType>&lt;&gt;</diffType>

**Operátor nerovnosti <>. Značí že soubor byl modifikován.**

<value1>2006-01-30T18:17:14.4266190</value1>

<value2>2006-01-30T18:23:22.6968304</value2>

</Values>

<Values>

<name>fileAttributes</name>

**Atributy souboru.**

<diffType>=</diffType>

**Operátor rovnosti =. Značí že atributy souboru nebyly modifikovány.**

<value1>32</value1>

<value2>32</value2>

</Values>

<Values>

<name>fileCreationTime</name>

**Datum vytvoření souboru. Značí že soubor byl modifikován.**

<diffType>=</diffType>

**Operátor rovnosti =. Značí že datum vytvoření souboru nebylo modifikováno.**

<value1>2006-01-30T18:15:52.6338534</value1>

**Datum vytvoření souboru.**

<value2>2006-01-30T18:15:52.6338534</value2>

**Datum vytvoření souboru.**

</Values>

<ACEs>

**Access Control Entry**

<user>

<userName>DOMENA\STANICE</userName>

**Jméno stanice**

<sid>S-1-5-21-591665024-1611875846-1847928074-1010</sid>

**Bezpečnostní identifikační číslo.**

</user>

<diffType>=</diffType>

**Operátor rovnosti =. značí že ACE u DOMENA\STANICE nebylo modifikováno.**

<ace1>Allow:rd|wd|ad|re|we|ex|dc|ra|ea</ace1>

<ace2>Allow:rd|wd|ad|re|we|ex|dc|ra|ea</ace2>

</ACEs>

</objectOS>

</ScanDiff>

</ScanDiffList>

## 6. Sledování služeb OS

### 6.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.**

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.**

```
<scanner>  
<scan id="scantest">  
  <services scanDrivers="0" scanServices="1" />  
</scan>
```

**Identifikuje scan jako "scantest". Hodnota "1" atributu scanServices zapíná sledování služeb.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

## 6.2 Příklady výstupních souborů

### 6.2.1 ScanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

```
</station>
```

#### **Scan1.**

```
<scan1>
```

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T17:24:20.5270000+01:00</scanDate>
```

```
</scan1>
```

#### **Scan2.**

```
<scan2>
```

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T17:40:59.9630000+01:00</scanDate>
```

```
</scan2>
```

```
<objectOS>
```

```
<name>SysKoTestSvc</name>
```

#### **Jméno služby.**

```
<type>service</type>
```

#### **Sledovaný typ - služba.**

```
<Values>
```

```
<name>serviceDisplayName</name>
```

```
<diffType>=</diffType>
```

```

    <value1>SysKoTestSvc</value1>
    <value2>SysKoTestSvc</value2>
  </Values>
</Values>
  <name>serviceType</name>
  <diffType>=</diffType>
  <value1>16</value1>
  <value2>16</value2>
</Values>
</Values>
  <name>serviceStatus</name>
  <diffType>&lt;&gt;</diffType>

```

#### **Operátor nerovnosti <>. Značí změnu stavu služby.**

```

    <value1>1</value1>
    <value2>4</value2>
  </Values>
</objectOS>
</ScanDiff>
</ScanDiffList>

```

### **6.2.2 ScanList**

Obsahem notifikace ScanList je seznam scanu.

```

<ScanList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <scan>
    <stationID>192.168.168.15</stationID>

```

#### **IP adresa stanice.**

```

  <scanID>scantest</scanID>

```

**ID scanu.**

```
<scanDate>2006-01-30T17:24:20.5270000+01:00</scanDate>
```

**Datum scanu.**

```
<scanResult>OK</scanResult>
```

**Výsledek scanu.**

```
</scan>
```

```
</ScanList>
```

### 6.2.3 StationList

Seznam stanic které se kdy připojily.

```
<Stations xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<station>
```

```
<id>192.168.168.15</id>
```

**IP adresa stanice.**

```
<publicAddress>192.168.168.15</publicAddress>
```

**Veřejná IP adresa stanice.**

```
</station>
```

```
</Stations>
```

## 7. Sledování registrů

### 7.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.**

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL tcp://localhost:10082/SysKoManager.**

```
<scanner>
```

```
<scan id="scantest">
```

```
<registry name="LocalMachine\Software\SysKo" recursive="1" />
```

```
</scan>
```

**Identifikuje scan jako "scantest". Atribut name definuje "LocalMachine\Software\SysKo" jako sledovanou větev v registrech. Hodnota "1" atributu recursive zapíná sledování podřízených větví registru.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

## 7.2 Příklad výstupního souboru scanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

**IP adresa sledované stanice.**

```
</station>
```

```
<scan1>
```

**Scan1.**

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:27:53.3600000+01:00</scanDate>
```

```
</scan1>
```

```
<scan2>
```

**Scan2.**

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:28:09.7970000+01:00</scanDate>
```

```
</scan2>
```

```
<objectOS>
```

```
<name>HKEY_LOCAL_MACHINE\Software\SysKo</name>
```

**Sledovaná větev v registru.**

```
<type>registry</type>
```

```
<Values>
```

```
<name>HKEY_LOCAL_MACHINE\Software\SysKo\StringValue</name>
```

**Změna hodnoty položky StringValue.**

```
<diffType>&lt;&gt;</diffType>
```

```
<value1>2</value1>
```

```
<value2>3</value2>
```

```
</Values>
```

```
</objectOS>
```

```
</ScanDiff>
```

```
</ScanDiffList>
```

## 8. Sledování bezpečnostní politiky

### 8.1 Příklad nastavení konfiguračního souboru

```
<configuration>
```

**Sekce <configSections> není určena k nastavení uživatelských parametrů systému.**

```
<configSections>
```

```
<sectionGroup name="SysKo">
```

```
<section name="appSettings"  
type="Wak.Wnt.As.AppConfigurationSettingsConfigurationSectionHandler, Wak.Wnt.As" />
```

```
<section name="scanner" type="Wak.SysKo.As.Client.ScannerConfigurationSectionHandler,  
Wak.SysKo.As.Client" />
```

```
<section name="eventLog"  
type="Wak.SysKo.As.Client.EventLogConfigurationSectionHandler, Wak.SysKo.As.Client"  
/>
```

```
</sectionGroup>
```

```
</configSections>
```

**Zde začíná sekce <Sysko>, ta je určena k nastavení uživatelských parametrů systému.**

```
<SysKo>
```

```
<appSettings remoteManager="true"  
remoteManagerUrl="tcp://localhost:10082/SysKoManager" />
```

**Element <appSetting> definuje použití remoteManageru na URL  
tcp://localhost:10082/SysKoManager.**

```
<scanner>  
<scan id="scantest">  
  <policy exclude="^\signature$" />  
</scan>
```

**Identifikuje scan jako "scantest". Element <policy> definuje sledování bezpečnostní politiky. Ze sledování je vyloučena bezpečnostní politika jejíž název odpovídá regulárnímu výrazu ^\signature\$.**

```
</scanner>
```

```
</SysKo>
```

```
</configuration>
```

## 8.2 Příklad výstupního souboru scanDiff

```
<ScanDiffList xmlns:xsd="http://www.w3.org/2001/XMLSchema"  
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

```
<ScanDiff>
```

```
<station>
```

```
<id>192.168.168.15</id>
```

### IP adresa sledované stanice.

```
</station>
```

```
<scan1>
```

#### scan1.

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:42:55.1130000+01:00</scanDate>
```

```
</scan1>
```

```
<scan2>
```

#### scan2.

```
<scanID>scantest</scanID>
```

```
<scanDate>2006-01-30T18:44:30.6970000+01:00</scanDate>
```

```
</scan2>
```

```
<objectOS>
```

```
<name>Policy</name>
```

```
<type>policy</type>
```

### Typ bezpečnostní politiky.

```
<Values>
```

```
<name>MinimumPasswordAge</name>
```

### Minimální stáří hesla

<diffType>=</diffType>

<value1>0</value1>

<value2>0</value2>

</Values>

<Values>

<name>MinimumPasswordLength</name>

### **Minimální délka hesla**

<diffType>&lt;&gt;</diffType>

### **Operátor nerovnosti <>, značí změnu.**

<value1>6</value1>

### **Stará minimální délka hesla**

<value2>5</value2>

### **Nová minimální délka hesla**

</Values>

</objectOS>

</ScanDiff>

</ScanDiffList>



# Obsah

<b>Úvod</b> .....	<b>1</b>
<b>1. Popis</b> .....	<b>1</b>
<b>2. Konfigurační soubor SysKoServer</b> .....	<b>2</b>
2.1 Příklad nastavení .....	2
<b>3. Nastavení kontroly BS7779</b> .....	<b>6</b>
<b>4. Sledování událostí</b> .....	<b>8</b>
4.1 Příklad nastavení konfiguračního souboru .....	8
4.2 Příklad výstupního souboru .....	9
<b>5. Sledování souborů</b> .....	<b>11</b>
5.1 Příklad nastavení konfiguračního souboru .....	11
5.2 Příklad výstupního souboru .....	12
<b>6. Sledování služeb OS</b> .....	<b>15</b>
6.1 Příklad nastavení konfiguračního souboru .....	15
6.2 Příklady výstupních souborů .....	16
<b>7. Sledování registrů</b> .....	<b>19</b>
7.1 Příklad nastavení konfiguračního souboru .....	19
7.2 Příklad výstupního souboru scanDiff .....	20
<b>8. Sledování bezpečnostní politiky</b> .....	<b>21</b>
8.1 Příklad nastavení konfiguračního souboru .....	21
8.2 Příklad výstupního souboru scanDiff .....	22

# Slovníky

## Zkratky

Zkratka	Význam
OS	Operační systém

Tab. 1 Slovník zkratk

## Termíny

Termín	Význam
Regulární výraz	Regulární výraz (regular expression) je speciální řetězec znaků, který představuje určitý vzor (masku) pro textové řetězce.
Reference	Vztah (odkaz) mezi dvěma elementy dokumentu.
Atribut	Atribut je označení datového prostoru, uchovávající datovou hodnotu. Je specifikován jménem, případně typem a rozsahem uchovávaných hodnot.
XML	Extensible Markup Language. Značkovací jazyk popisující strukturu dokumentu.
CSS	Cascading Style Sheet. Technologie pro přidávání stylu k webovým dokumentům.
SMTP	Simple Mail Transfer Protocol - jednoduchý protokol pro odesílání a přenos pošty mezi poštovními servery.
IP adresa	IP adresa je jedinečná adresa počítače. IP adresa se udává ve tvaru xxx.xxx.xxx.xxx, kde xxx je číslo v rozsahu 0 až 255. Může vypadat například takto: 127.0.0.1
makro	Je identifikováno uvozujícím a ukončujícím řetězcem "@@". Po vyhodnocení systémem je jeho hodnota nahrazena významem makra. Např. hodnotou makra @@WINDIR@@ může být řetězec "C:\WINNT".
ACE	Access Control Entry. Obsahuje množinu přístupových práv uživatele k danému objektu. Součástí je i bezpečnostní identifikátor.
notifikace	Odeslání reportu o sledovaných událostech. Podle nastavení je formou reportu soubor uložený na disk nebo odeslaný el. poštou.
localhost	Místní adresa právě používané stanice. Odpovídá IP adrese 127.0.0.1
Scan	Zjištění aktuálního stavu objektu.
URL	Uniform Resource Locator. URL je standardizovaný řetězec znaků identifikující zdroj a způsob přístupu k němu.

Tab. 2 Slovník termínů