



WAK System ®

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

Název zprávy:	Závěrečná zpráva projektu
Název části:	Systemová příručka
Období:	1.1.2005-31.12.2005

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

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

Datum vydání:	31.1.2006
---------------	------------------

Úvod

Systémová příručka popisuje syntaxi a význam jednotlivých nastavitelných položek konfiguračních souborů systému a význam položek výstupních sestav.




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.

Systém obsahuje tři konfigurační soubory, dva klientské (SysKoApp\App.config a SysKoConsole\App.config) a jeden serverový (SysKoServer\App.config). Pro kontrolu validity jsou k těmto XML souborům připojena odpovídající XML schémata (AppConfig.xsd).

Dále systém obsahuje 5 schémat ve formátu XSLT, s jejichž pomocí jsou vytvořeny příslušné výstupní sestavy.

V dalších kapitolách je popsán význam jednotlivých položek a jejich syntaxe pomocí XML schémat. Ve XML schématech jsou použity následující typy relací.

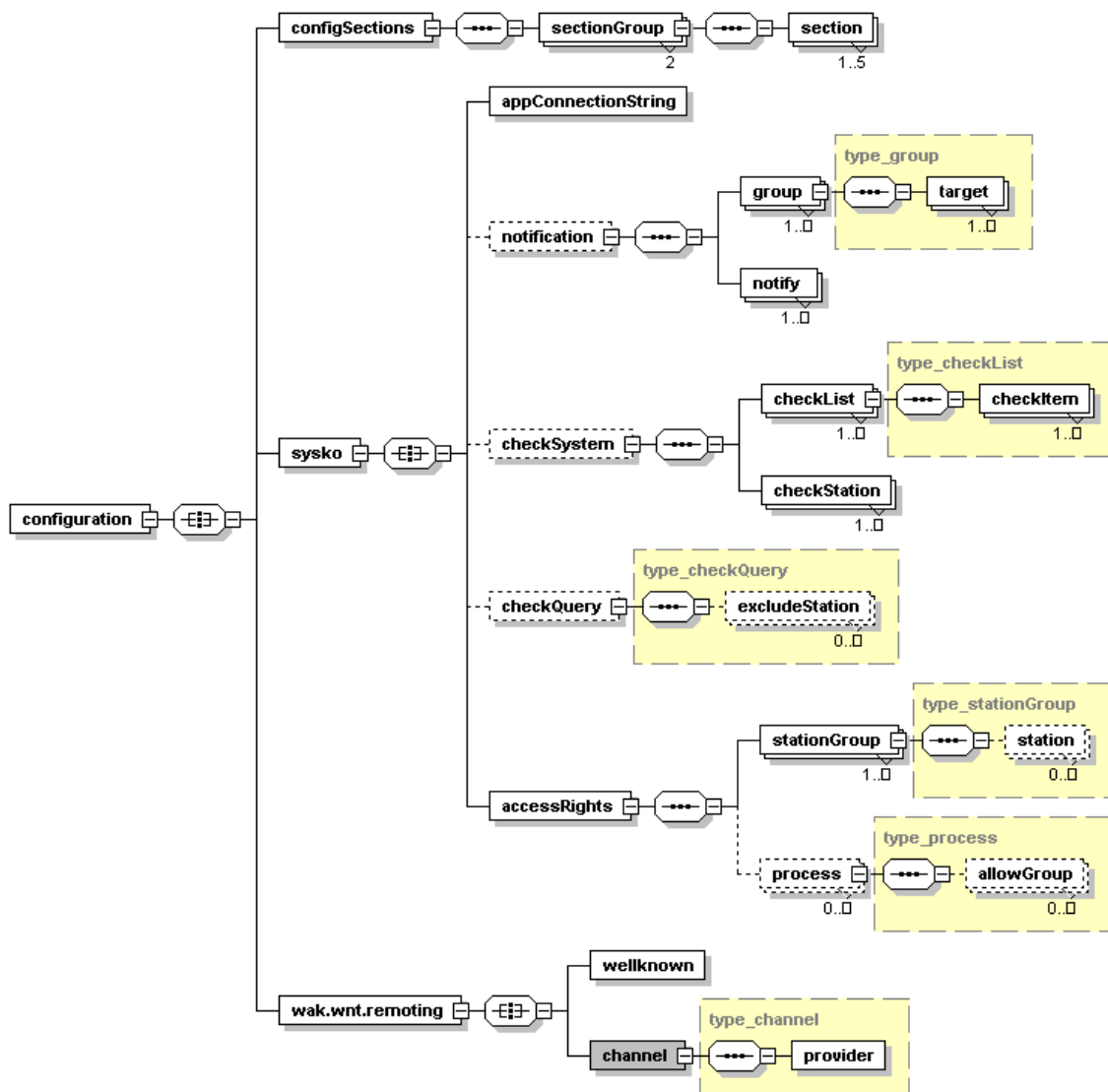
Seznam relací	Popis
	Vnořené elementy mohou být v libovolném pořadí.
	Vnořný element bude jeden z několika možných.
	Vnořené elementy musejí odpovídat specifikovanému pořadí.

Tab. 1 Relace XML schémat

2. Konfigurační soubory na straně serveru

2.1 Konfigurační soubor SysKoServer

Struktura konfiguračního souboru SysKoServer\App.config je určena XML schématem SysKoServerAppConfig.xsd.



Obr. 1 Hierarchie konfiguračního souboru SysKoServer

2.1.1 Element <configuration>

Název elementu: configuration

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element celého XML dokumentu.

2.1.2 Element <configSections>

Název elementu: configSections

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro samotný systém. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému.

2.1.3 Element <sysko>

Název elementu: sysko

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element pro nastavení uživatelských parametrů systému.

2.1.4 Element <appConnectionString>

Název elementu: appConnectionString

Atributy: string database, string server, string uid, string pwd

Min. výskyt: 1

Max. výskyt: 1

Popis:

Atributy tohoto elementu obsahují konfigurační údaje pro přihlášení k databázi. Atribut database určuje jméno databáze na serveru určeném atributem server. Atributy uid a pwd určují uživatelské jméno a heslo pro přístup k databázi.

2.1.5 Element <notification>

Název elementu: notification

Atributy: string xsltPath, string cssPath

Min. výskyt: 0

Max. výskyt: 1

Popis:

Atributy xsltPath a cssPath určují adresář se soubory s XSL transformací, resp. adresář s CSS styly. XSL transformace ve spojení s CSS stylem určuje výslednou podobu výstupní XHTML stránky (sestavy), která je generována systémem.

2.1.6 Element <group>

Název elementu: group

Atributy: string id, string smtpserver, string mailfrom, string directory

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Atribut id jednoznačně identifikuje skupinu tvořenou elementem <group>. Na takto identifikovanou skupinu se lze poté odkazovat pomocí hodnoty atributu sendTo v elementu <notify> viz. 2.1.9. Atribut smtpserver určuje SMTP server, který se použije pro odeslání notifikace z elektronické adresy mailfrom. Atribut directory určuje adresář na serveru pro ukládání notifikací. Atributy: smtpserver a mailfrom mají smysl pouze tehdy, je-li hodnotou atributu proto vnořeného elementu <target> (viz. 2.1.8) řetězec “smtp”. Je-li hodnotou atributu proto řetězec “file” má význam atribut directory.

2.1.7 Element <target>

Název elementu: target

Atributy: type_protokol proto, string xslt, string css, string name

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Atribut proto určuje způsob notifikace. Je-li hodnotou atributu proto řetězec “file”, výsledkem notifikace je XHTML stránka (sestava) uložená v adresáři specifikovaným atributem directory rodičovského elementu <group>. Je-li hodnotou atributu proto řetězec “smtp”, výsledkem notifikace je XHTML stránka (sestava), zasílaná na elektronickou adresu specifikovanou

atributem `directory` rodičovského elementu `<group>`. Atributy `xslt` a `css` specifikují soubor s XSL transformací, resp. s CSS stylem. Pro použití XSL transformace, resp. CSS stylu podle druhu notifikace, existuje možnost vložit do hodnot atributů `xslt` a `css` makro `@@ACTION@@`. Makro `@@ACTION@@` nabývá hodnot typu `type_action`, podle hodnoty atributu `action` referujícího elementu `<notify>`. Reference je realizována pomocí atributu `sendTo`. Takto jsou jednotlivé notifikace rozesílány skupinám identifikovaným atributem `id`. Atribut `name` určuje jméno souboru výsledné notifikace. V jeho těle lze použít makra `@@ACTION@@` a `@@DATE:type_dateFormat@@`. V řetězci `type_dateFormat` mají jednotlivé znaky speciální význam určující výsledný formát data, které je výstupem makra `@@DATE:type_dateFormat@@`, `type_dateFormat` je typu `string`.

Formátovací řetězec	Popis
“d”	Den v měsíci. Jednociferné dny nezačínají nulou.
“dd”	Den v měsíci. Jednociferné dny začínají nulou.
“dddd”	Název dne v týdnu.
“M”	Měsíc vyjádřen číslem. Jednociferné nezačínají nulou.
“MM”	Měsíc vyjádřen číslem. Jednociferné začínají nulou.
“MMMM”	Název měsíce.
“y”	Rok bez století. Jestliže je rok bez století menší než 10, je rok zobrazen bez nul na začátku.
“yy”	Rok bez století. Jestliže je rok bez století menší než 10, je rok zobrazen s nulami na začátku.
“yyyy”	Čtyřciferný rok, obsahující století.
“h”	Hodina v 12 hodinovém značení. Jednociferné nezačínají nulou.
“hh”	Hodina v 12 hodinovém značení. Jednociferné začínají nulou.
“H”	Hodina v 24 hodinovém značení. Jednociferné nezačínají nulou.
“HH”	Hodina v 24 hodinovém značení. Jednociferné začínají nulou.
“m”	Minuta. Jednociferná nezačíná nulou.
“mm”	Minuta. Jednociferná začíná nulou.
“s”	Sekunda. Jednociferná nezačíná nulou.
“ss”	Sekunda. Jednociferná začíná nulou.
“T”	Desetina sekundy

Tab. 2 Význam speciálních znaků v řetězci `type_dateFormat`

2.1.8 Element `<notify>`

Název elementu: `notify`

Atributy: `string id`, `type_action action`, `string stationID`, `string sendTo`,
`unsignedInt interval`

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <notify> určuje typ notifikace, která se bude posílat skupině definované pomocí elementu <group>. Umožňuje nastavit délku periody, v níž bude docházet k notifikacím, a specifikovat stanice, které mají být obsahem notifikace.

Atribut id je jedinečným identifikátorem elementu. Atribut action určuje typ notifikace, ve spojení se stationID specifikuje stanice a typ reportu, které jsou předmětem notifikace. Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice. Atribut sendTo odkazuje na cíl notifikace. Tím je skupina definována elementem <group> s jedinečným identifikátorem atributem id. Periodicitu notifikací stanovuje atribut interval, doba periody je udávána v minutách. Je-li hodnota atributu interval rovna nule, je notifikace vypnuta.

2.1.9 Element <checkSystem>

Název elementu: checkSystem

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <checkSystem> obsahuje seznam testů, definovaných v elementech <checkList> a vazby jednotlivých testů na seznam stanic, které jsou definovány v elementech <checkStation>.

2.1.10 Element <checkList>

Název elementu: checkList

Atributy: string id, type_logOp logOp

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkList> obsahuje seznam kontrolovaných položek, definovaných v elementech <checkItem>.

Atribut id je jedinečným identifikátorem elementu <checkList>. Logický operátor logOp stanovuje, stačí-li pro úspěšný test splnit pouze jednu podmínku, nebo je nutno splnit všechny. Je-li hodnotou operátoru “and”, je nutno splnit všechny podmínky definované elementy <checkItem>. Je-li hodnotou operátoru “or”, stačí splnit pouze jednu podmínku. Implicitní hodnota operátoru logOp je “and”.

2.1.11 Element <checkItem>

Název elementu: checkItem

Atributy: string id, type_type type, string name, type_operator op, string value

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkItem> popisuje typ a způsob kontroly položky.

Atribut id je jedinečným identifikátorem elementu <checkItem>. Atribut type a name specifikuje typ testované položky, resp. její název. Hodnota atributu op funguje jako operátor mezi operandem value a operandem tvořeným hodnotou položky name.

Hodnotou atributu name mohou být makra @@WINDIR@@, @@SYSTEMDRIVE@@, @@SYSTEMROOT@@ a @@PROGRAMFILES@@. Jejich hodnotami jsou potom odpovídající hodnoty prostředí tak, jak jsou nastaveny v OS.

Hodnotou atributu value může být makro @@TODAY@@, jeho hodnotou je potom aktuální datum. Je-li hodnotou atributu value makro @@TODAY@@, může být zapsáno ve tvaru @@TODAY@@+počet_dnů, resp. @@TODAY@@-počet_dnů, kde počet_dnů je typu unsignedInt a představuje časový posun od aktuálního data v jednotkách dnů.

2.1.12 Element <checkStation>

Název elementu: checkStation

Atributy: string stationID, string checkList

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkStation> umožňuje asociovat a slučovat testy definované elementem <checkList> s libovolnými stanicemi.

Atribut id je jedinečným identifikátorem elementu <checkStation>. Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice, pro níž se provedou testy specifikované atributem checkList. V atributu checkList lze vyjmenovat více testů a spojit je ve tvaru test1|test2, kde znak '|' je oddělovač typu type_itemSeparator.

2.1.13 Element <checkQuery>

Název elementu: checkQuery

Atributy: type_portNumber port

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <checkQuery> definuje UDP port služby CheckQuery.

2.1.14 Element <excludeStation>

Název elementu: excludeStation

Atributy: string stationID

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <excludeStation> definuje stanice, které mohou využívat služby CheckQuery.

Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice, která má přístup k službě CheckQuery.

2.1.15 Element <accessRights>

Název elementu: accessRights

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <accessRights> obsahuje definici skupin stanic a jejich práv pro přístup k jednotlivým procesům systému.

2.1.16 Element <stationGroup>

Název elementu: stationGroup

Atributy: string id

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <stationGroup> obsahuje seznam stanic, definovaných pomocí vnořeného elementu <station>.

Atribut id je jedinečným identifikátorem elementu.

2.1.17 Element <station>

Název elementu: station

Atributy: string stationID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <station> definuje stanice, které jsou součástí skupiny rodičovského elementu <stationGroup>.

Hodnotou atributu stationID je regulární výraz popisující IP adresu stanice.

2.1.18 Element <process>

Název elementu: process

Atributy: string typeID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <process> identifikuje proces systému, k němuž mají přístup stanice definované vnořeným elementem <allowGroup>.

Atribut typeID identifikuje proces systému.

2.1.19 Element <allowGroup>

Název elementu: allowGroup

Atributy: string groupID

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <allowGroup> definuje skupinu stanic, které mají možnost přístupu k procesu systému identifikovaného atributem typeID vnějšího elementu <process>.

Hodnotou atributu groupID je identifikátor elementu <stationGroup>.

2.1.20 Element <wak.wnt.remoting>

Název elementu: wak.wnt.remoting

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro běh samotného systému. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému, vyjma vnořeného elementu <channel>.

2.1.21 Element <channel>

Název elementu: channel

Atributy: string ref, type_portNumber port

Min. výskyt: 1

Max. výskyt: 1

Popis:

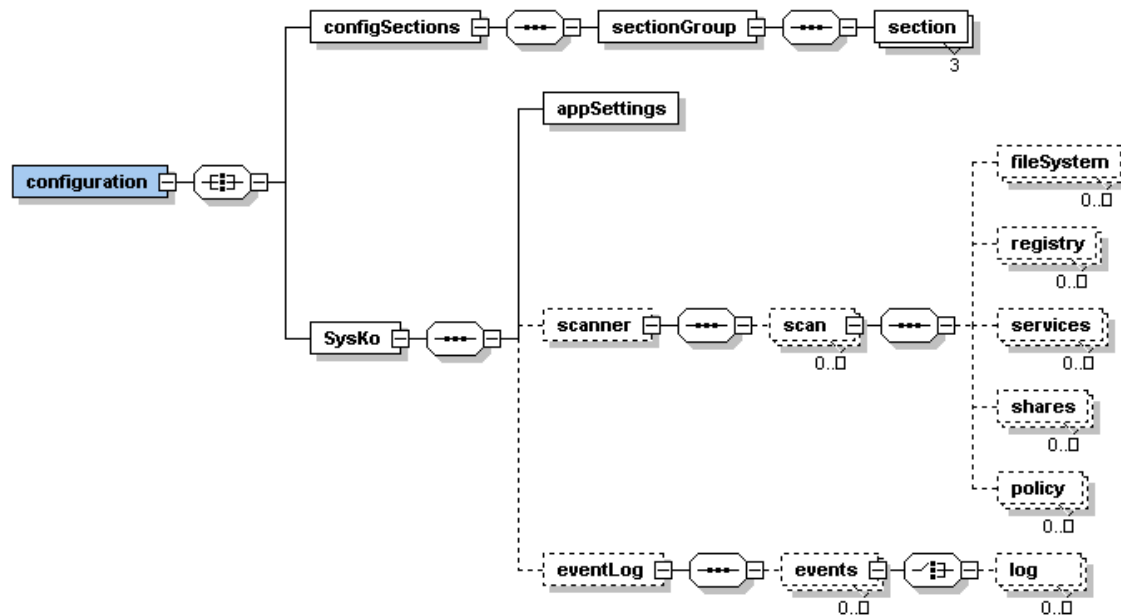
Element <channel> definuje komunikační protokol a číslo portu, na kterém probíhá komunikace mezi klientem a serverem.

Atribut ref definuje komunikační protokol. Atribut port definuje číslo portu.

2.2 Konfigurační soubory na straně klienta

2.2.1 Konfigurační soubor SysKoConsole

Struktura konfiguračního souboru SysKoConsole\App.config je určena XML schématem SysKoConsoleAppConfig.xsd.



Obr. 2 Hierarchie konfiguračního souboru SysKoConsole

2.2.2 Element <configuration>

Název elementu: configuration

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element celého XML dokumentu.

2.2.3 Element <configSections>

Název elementu: configSections

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Tento element obsahuje konfigurační údaje nutné pro samotný systém. Tato sekce není určena k modifikaci pro nastavení uživatelských parametrů systému.

2.2.4 Element <sysko>

Název elementu: sysko

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Kořenový element pro nastavení uživatelských parametrů systému.

2.2.5 Element <appSettings>

Název elementu: appSettings

Atributy: type_bool remoteManager, string remoteManagerUrl

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <appSetting> definuje použití a URL vzdálené služby manažeru.

Atribut remoteManager definuje přítomnost vzdálené služby manažeru. Je-li hodnotou řetězec “true”, je použita vzdálená služba manažeru lokalizována URL adresou atributu remoteManagerUrl.

2.2.6 Element <scanner>

Název elementu: scanner

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <scanner> obsahuje seznam jednotlivých testů definovaných pomocí vnořených elementů <scan>.

2.2.7 Element <scan>

Název elementu: scan

Atributy: string id

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <scan> reprezentuje jeden test. Test je definovaný vnořenými elementy, které specifikují položky jež jsou předmětem testu.

Atribut id je jedinečný identifikátor elementu <scan>.

2.2.8 Element <fileSystem>

Název elementu: fileSystem

Atributy: string name, type_boolInt recursive, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <fileSystem> specifikuje cestu v lokálním souborovém systému a způsob vyhledávání.

Atribut name specifikuje cestu v lokálním souborovém systému. Atribut recursive definuje testování podadresářů. Je-li jeho hodnotou "1", jsou testovány i podadresáře na cestě definované atributem name. Hodnotou atributu exclude je regulární výraz popisující jména souborů, která nemají být zahrnuty do testu.

2.2.9 Element <registry>

Název elementu: registry

Atributy: string name, type_boolInt recursive, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <registry> specifikuje větev v systémovém registru OS a způsob vyhledávání.

Atribut name specifikuje větev v systémovém registru OS. Atribut recursive definuje testování podřízených větví. Je-li jeho hodnotou "1", jsou testovány i podřízené větve na cestě definované atributem name. Hodnotou atributu exclude je regulární výraz popisující klíče, které nemají být zahrnuty do testu.

2.2.10 Element <services>

Název elementu: services

Atributy: type_boolInt scanDrivers, type_boolInt scanServices, string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <services> specifikuje testování ovladačů a služeb systému.

Atribut scanDrivers definuje testování ovladačů OS. Je-li hodnotou atributu scanDrivers “1”, ovladače OS jsou testovány, při hodnotě “0” ovladače OS nejsou testovány. Atribut scanServices definuje testování služeb OS. Je-li hodnotou atributu scanServices “1”, služby OS jsou testovány, při hodnotě “0” služby OS nejsou testovány. Hodnotou atributu exclude je regulární výraz popisující název služby nebo ovladače, které nemají být zahrnuty do testu.

2.2.11 Element <shares>

Název elementu: shares

Atributy: string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <shares> specifikuje testování sdílených prostředků OS.

Hodnotou atributu exclude je regulární výraz popisující název sdíleného prostředku, který nemá být zahrnut do testu.

2.2.12 Element <policy>

Název elementu: policy

Atributy: string exclude

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <policy> specifikuje testování bezpečnostní politiky OS.

Hodnotou atributu exclude je regulární výraz popisující název bezpečnostní politiky, která nemá být zahrnuta do testu.

2.2.13 Element <eventLog>

Název elementu: eventLog

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <eventLog> obsahuje seznam jednotlivých sestav mapujících události definované pomocí vnořených elementů <event>.

2.2.14 Element <events>

Název elementu: events

Atributy: string id

Min. výskyt: 0

Max. výskyt: neomezen

Popis:

Element <events> reprezentuje jednu sestavu. Sestava je definována vnořenými elementy, které specifikují položky jež jsou mapovány.

Atribut id je jedinečný identifikátor elementu <events>.

2.2.15 Element <log>

Název elementu: events

Atributy: string name, string machine, string dateFrom, string dateTo

string type, string source, string ID, string userName

Min. výskyt: 0

Max. výskyt: neomezen

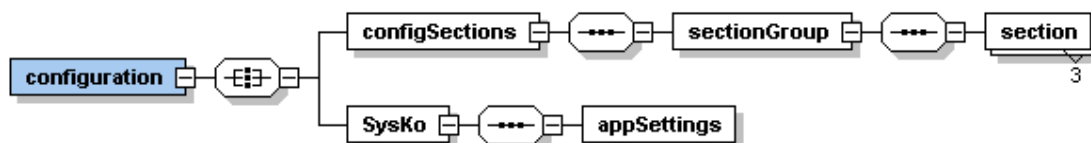
Popis:

Element <log> specifikuje události určené k monitorování.

Volitelné atributy elementu <log> popisují, jaké parametry musí událost splňovat. Atribut name označuje druh protokolu události. Možné hodnoty jsou “system” a “application”, případně jejich kombinace zapsaná pomocí type_itemSeparator. Atribut machine označuje jméno počítače. Atribut dateFrom a dateTo stanovují, v jakém časovém intervalu událost vznikla. Atribut type určuje typ události. Možné hodnoty jsou “Information”, “Error”, “FailureAudit”, “Warning” a “SuccessAudit”. Atribut source označuje zdroj události. Atribut ID je identifikačním číslem události. Atribut userName označuje jméno uživatelského účtu, pod kterým došlo k události.

2.3 Konfigurační soubor SysKoApp

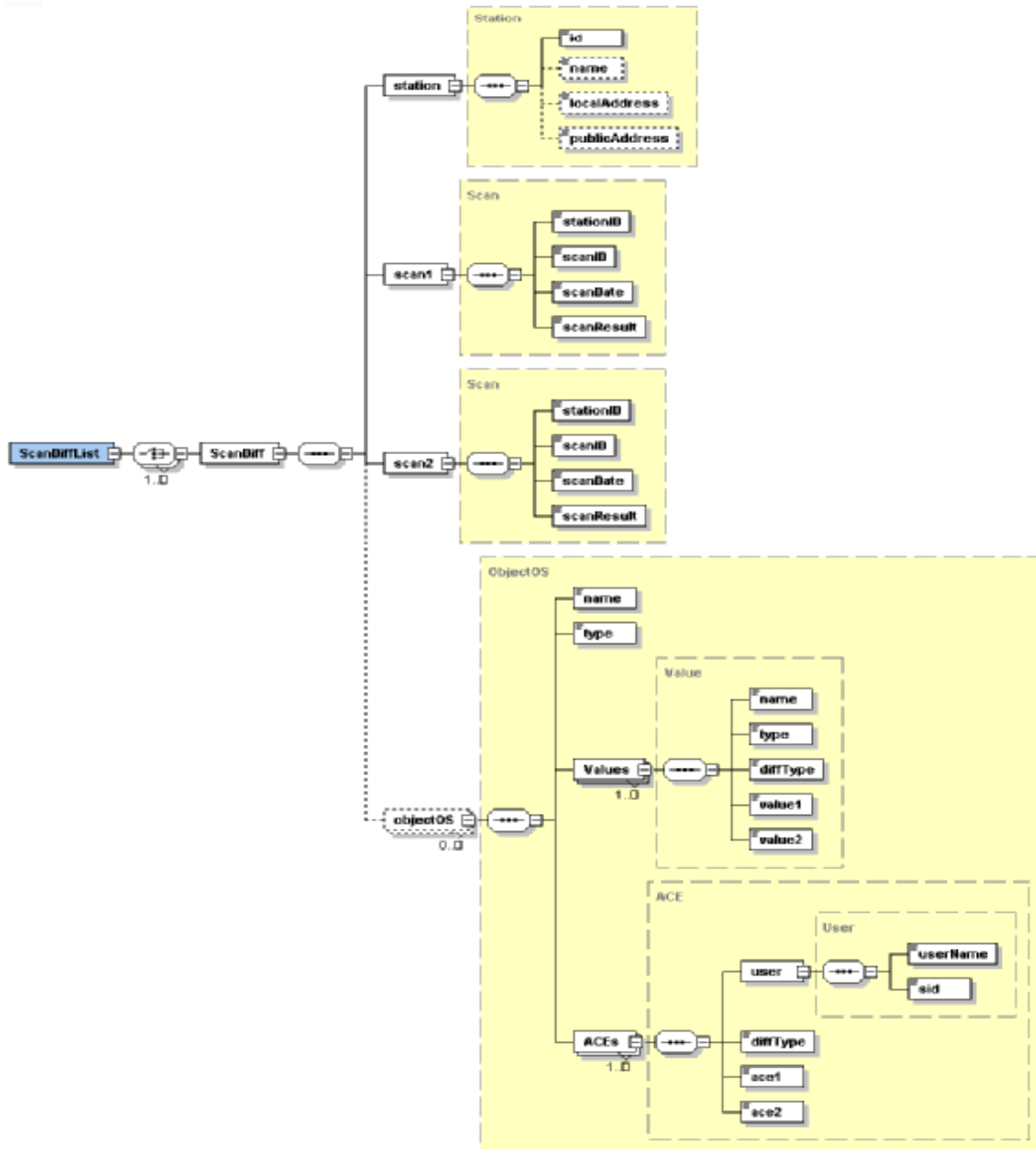
Struktura konfiguračního souboru SysKoApp\App.config je určena XML schématem SysKoConsoleAppConfig.xsd. Hodnoty elementů se v tomto konfiguračním souboru nenastavují.



Obr. 3 Hierarchie konfiguračního souboru SysKoApp

3. Výstupní soubory

3.1 scanDiff



Obr. 4 Schéma výstupního souboru scanDiff

ScanDiff popisuje vzniklé diference mezi scan1 a scan2. Struktura výstupního souboru scanDiff je určena XML schématem scanDiff.xsd.

3.1.1 Element <scanDiffList>

Název elementu: scanDiffList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDiffList> je kořenovým elementem výstupu scanDiff.

3.1.2 Element <scanDiff>

Název elementu: scanDiff

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDiff> popisuje pomocí vnořených elementů diference dvou bezpečnostních kontrol.

3.1.3 Element <station>

Název elementu: station

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <station> je typu Station. Specifikuje stanici u které byla zapnuta notifikace typu scanDiff.

3.1.4 Element <scan1>

Název elementu: scan1

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan1> je typu Scan, představuje referenční scan, ke kterému se změny vztahují.

3.1.5 Element <scan2>

Název elementu: scan2

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan2> je typu Scan, představuje porovnávaný scan vůči vzoru.

3.1.5.1 Element <objectOS>

Název elementu: objectOS

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <objectOS> uchovává informace o změně.

3.1.6 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <name> označuje položku změny.

3.1.7 Element <type>

Název elementu: type

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <type> označuje typ položky změny a nabývá hodnot typu type_type.

3.1.8 Element <Values>

Název elementu: Values

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <Values> je typu type_Value. Jeho vnořené elementy popisují změnu hodnoty. Element <name> znamená jméno položky, <type> je typ položky, <diffType> představuje typ změny, <value1> představuje původní hodnotu a <value2> hodnotu po změně.

3.1.9 Element <ACEs>

Název elementu: Values

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

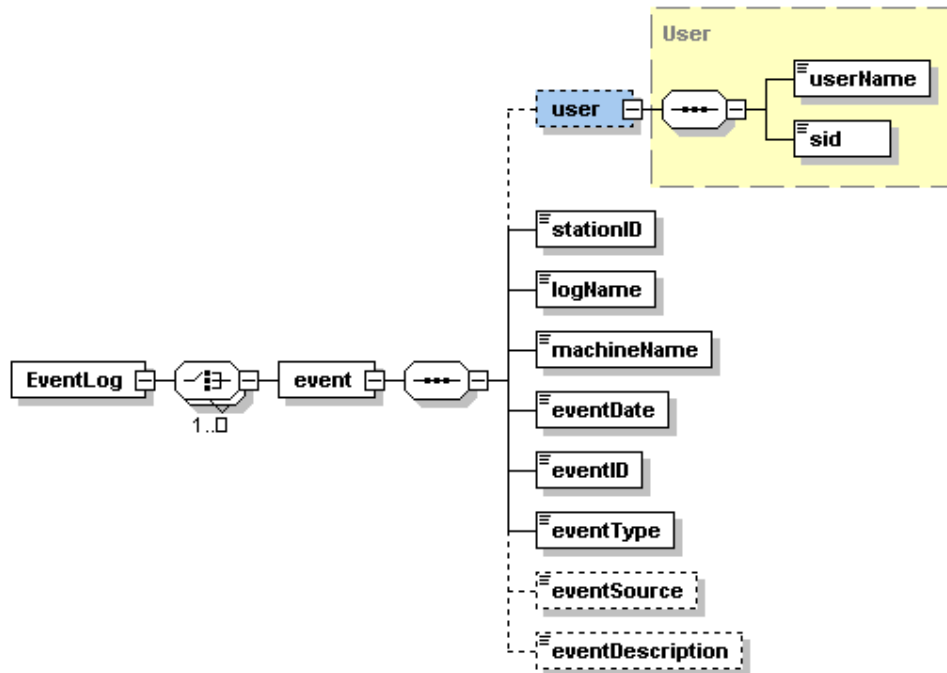
Popis:

Element <ACEs> je typu type_ACE. Jeho vnořené elementy popisují změnu hodnot ACE (access control entry), pro uživatele identifikovaného elementem <user>. Element <ace1> znamená hodnotu ACE před změnou, <ace2> hodnotu ACE po změně. Element <diffType> představuje typ změny.

3.2 EventLog

3.2.1 Hierarchie elementů

Struktura výstupního souboru eventLog je určena XML schématem eventLog.xsd.



Obr. 5 Schéma výstupního souboru eventLog

3.2.2 Element <EventLog>

Název elementu: EventLog

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <EventLog> je kořenový element výstupu EventLog.

3.2.3 Element <event>

Název elementu: event

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <event> pomocí vnořených elementů popisuje jednu událost.

3.2.4 Element <user>

Název elementu: user

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <user> identifikuje uživatele.

3.2.5 Element <stationID>

Název elementu: stationID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <stationID> obsahuje ID stanice.

3.2.6 Element <logName>

Název elementu: logName

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <logName> obsahuje jméno logu.

3.2.7 Element <machineName>

Název elementu: machineName

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <machineName> obsahuje jméno počítače.

3.2.8 Element <eventDate>

Název elementu: eventDate

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventDate> obsahuje datum události.

3.2.9 Element <eventID>

Název elementu: eventID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventID> identifikuje událost.

3.2.10 Element <eventType>

Název elementu: eventType

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventType> obsahuje typ události.

3.2.11 Element <eventSource>

Název elementu: eventSource

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <eventSource> identifikuje zdroj události.

3.2.12 Element <eventDescription>

Název elementu: eventDescription

Atributy: žádné

Min. výskyt: 1

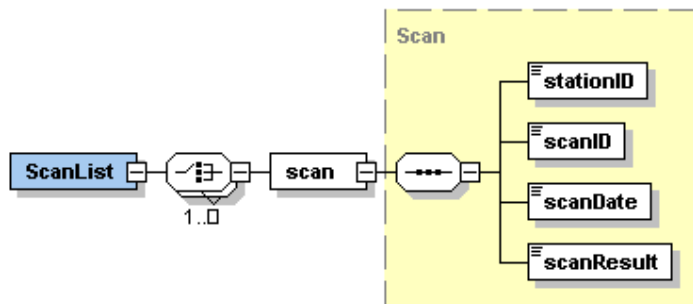
Max. výskyt: 1

Popis:

Element <eventDescription> obsahuje detailnější popis události.

3.3 scanList

3.3.1 Hierarchie elementů



Obr. 6 Schéma výstupního souboru scanList

Struktura výstupního souboru scanList je určena XML schématem scanList.xsd.

3.3.2 Element <scanList>

Název elementu: scanList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanList> je kořenovým elementem výstupu scanList.

3.3.3 Element <scan>

Název elementu: scan

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan> popisuje pomocí vnořených elementů jeden scan.

3.3.4 Element <stationID>

Název elementu: stationID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <stationID> identifikuje stanici, na které proběhl scan.

3.3.5 Element <scanID>

Název elementu: scanID

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanID> je identifikátorem scanu.

3.3.6 Element <scanDate>

Název elementu: scanDate

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scanDate> obsahuje datum scanu.

3.3.7 Element <scanResult>

Název elementu: scanResult

Atributy: žádné

Min. výskyt: 1

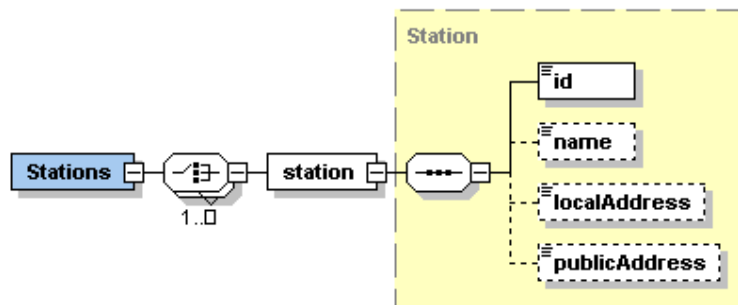
Max. výskyt: 1

Popis:

Element <scanResult> obsahuje výsledek scanu.

3.4 Stations

Struktura výstupního souboru stations je určena XML schématem stations.xsd.



Obr. 7 Schéma výstupního souboru Stations

3.4.1 Element <Stations>

Název elementu: Stations

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <Stations> je kořenovým elementem výstupu Stations.

3.4.2 Element <station>

Název elementu: station

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <station> popisuje pomocí vnořených elementů jednu stanici.

3.4.3 Element <id>

Název elementu: id

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <id> identifikuje stanici.

3.4.4 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <name> obsahuje jméno stanice.

3.4.5 Element <localAddress>

Název elementu: localAddress

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <localAddress> obsahuje lokální adresu stanice.

3.4.6 Element <publicAddress>

Název elementu: publicAddress

Atributy: žádné

Min. výskyt: 0

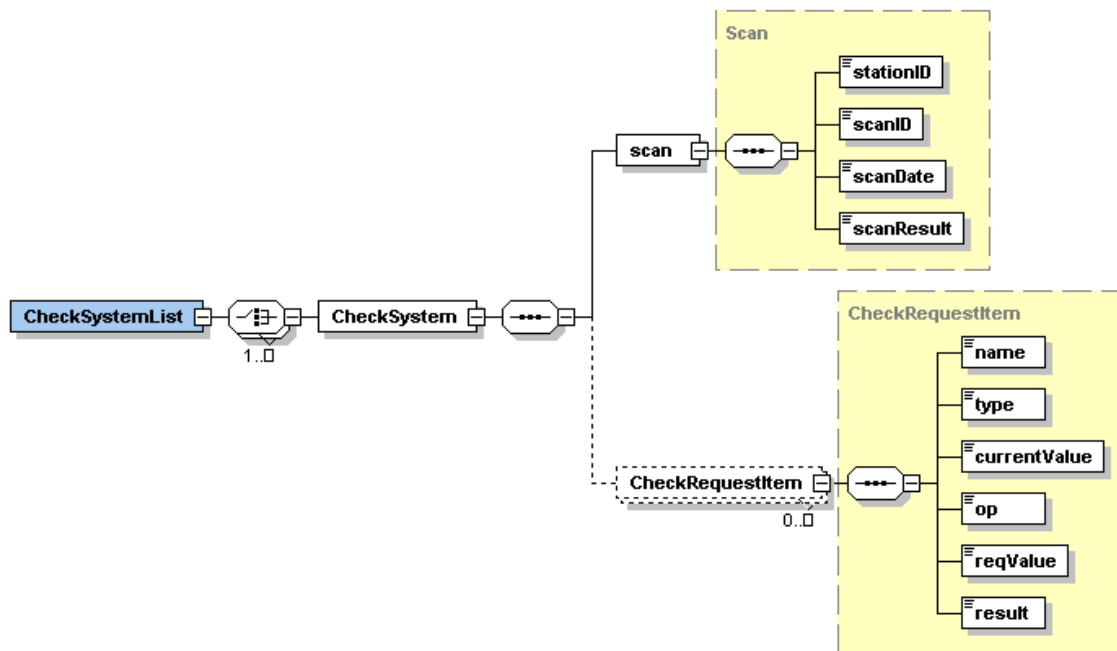
Max. výskyt: 1

Popis:

Element <publicAddress> obsahuje veřejnou adresu stanice.

3.5 CheckSystemList

Struktura výstupního souboru checkSystemList je určena XML schématem checkSystemList.xsd.



Obr. 8 Schéma výstupního souboru checkSystemList

3.5.1 Element <CheckSystemList>

Název elementu: CheckSystemList

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <CheckSystemList> je kořenovým elementem výstupu CheckSystemList.

3.5.2 Element <CheckSystem>

Název elementu: checkSystem

Atributy: žádné

Min. výskyt: 1

Max. výskyt: neomezen

Popis:

Element <checkSystem> popisuje pomocí vnořených elementů výsledek kontroly CheckSystem.

3.5.3 Element <scan>

Název elementu: scan

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <scan> popisuje pomocí vnořených elementů jeden scan.

3.5.4 Element <checkRequestItem>

Název elementu: checkRequestItem

Atributy: žádné

Min. výskyt: 0

Max. výskyt: 1

Popis:

Element <checkRequestItem> popisuje výsledek kontroly definované elementem <checkItem>.

3.5.5 Element <name>

Název elementu: name

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <name> obsahuje jméno testované položky.

3.5.6 Element <type>

Název elementu: type

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <type> obsahuje typ testované položky.

3.5.7 Element <currentValue>

Název elementu: currentValue

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <currentValue> obsahuje současnou hodnotu testované položky.

3.5.8 Element <op>

Název elementu: op

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <op> obsahuje operátor aplikovaný na currentValue a reqValue.

3.5.9 Element <reqValue>

Název elementu: reqValue

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <reqValue> obsahuje požadovanou hodnotu testované položky.

3.5.10 Element <result>

Název elementu: result

Atributy: žádné

Min. výskyt: 1

Max. výskyt: 1

Popis:

Element <result> obsahuje výsledek porovnávání obsahů elementů <reqValue> a <currentValue> pomocí operátoru definovaného v elementu <op>.

4. Seznam typů a struktur

4.1 Základní datové typy

Typ	Popis	Příklad
String	řetězec znaků	Abc
UnsignedInt	nezáporné celé číslo, číslo je v rozsahu od 0 do 4294967295, což odpovídá 32bitovému celému číslu	7, 657
DateTime	datum a čas	2005-07-05T10:58:53+02:00, 2005-07-05T08:58:53Z

Tab. 3 Základní použité datové typy

4.2 Jednoduché odvozené typy

Jednoduché odvozené typy jsou definovány restrikcí základních datových typů definovaných v kapitole 4.1.

4.2.1 Jednoduché typy použité v konfiguračních souborech

4.2.1.1 type_protokol

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot "smtp" a "file".

4.2.1.2 type_portType

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot "tcp" a "udp".

4.2.1.3 type_action

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “stationList”, “eventLog”, “scanList”, “scanDiff” a “checkSystem”.

4.2.1.4 type_type

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “policy”, “file”, “registry”, “service” a “share”.

4.2.1.5 type_operator

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “=”, “>”, “>=”, “<”, “<=”, “date_>”, “date_>=”, “date_<” “date_<=”, “date_>”, “ver_>”, “ver_>=”, “ver_<”, “ver_<=” a “exists”.

4.2.1.6 type_portNumber

Numerický typ, vzniklý restrikcí typu unsignedInt.

Může nabývat numerické hodnoty v intervalu 1024 až 65535 včetně.

4.2.1.7 type_logOp

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “or” a “and”.

4.2.1.8 type_itemSeparator

Výčtový typ, vzniklý restrikcí typu string.

Je definován hodnotou “|”.

4.2.1.9 type_bool

Výčtový typ, vzniklý restrikcí typu string.

Může nabývat hodnot “true” a “false”.

4.2.1.10 type_boolInt

Numerický typ, vzniklý restrikcí typu unsignedInt.

Může nabývat numerických hodnot 0 a 1.

4.3 Komplexní typy

Komplexní typy definují strukturu typů za pomoci výčtu atributů, podřízených elementů a jejich relací.

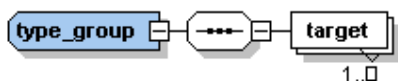
4.3.1 Komplexní typy použité v konfiguračních souborech

4.3.1.1 type_section

Definuje množinu atributů.

4.3.1.2 type_group

Definuje množinu atributů a relaci.



Obr. 9 Typ relace mezi type_group a target

4.3.1.3 type_target

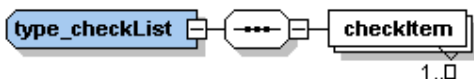
Definuje množinu atributů.

4.3.1.4 type_notify

Definuje množinu atributů.

4.3.1.5 type_checkList

Definuje množinu atributů a relaci.



Obr. 10 Typ relace mezi type_checklist a checkItem

4.3.1.6 type_checkItem

Definuje množinu atributů.

4.3.1.7 type_stationID

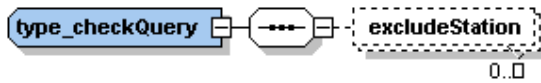
Definuje množinu atributů.

4.3.1.8 type_checkStation

Definuje množinu atributů.

4.3.1.9 type_checkQuery

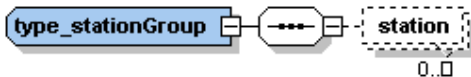
Definuje množinu atributů a relací.



Obr. 11 Typ relace mezi type_checkQuery a excludeStation

4.3.1.10 type_stationGroup

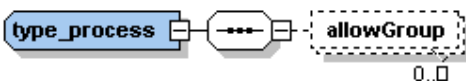
Definuje množinu atributů a relací.



Obr. 12 Typ relace mezi type_stationGroup a station

4.3.1.11 type_process

Definuje množinu atributů a relací.



Obr. 13 Typ relace mezi type_process a allowGroup

4.3.1.12 type_allowGroup

Definuje množinu atributů.

4.3.1.13 type_wellknown

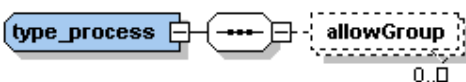
Definuje množinu atributů.

4.3.1.14 type_provider

Definuje množinu atributů.

4.3.1.15 type_process

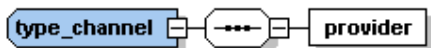
Definuje množinu atributů a relací.



Obr. 14 Typ relace mezi type_process a allowGroup

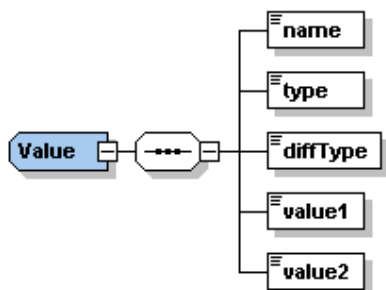
4.3.1.16 type_channel

Definuje množinu atributů a relací.



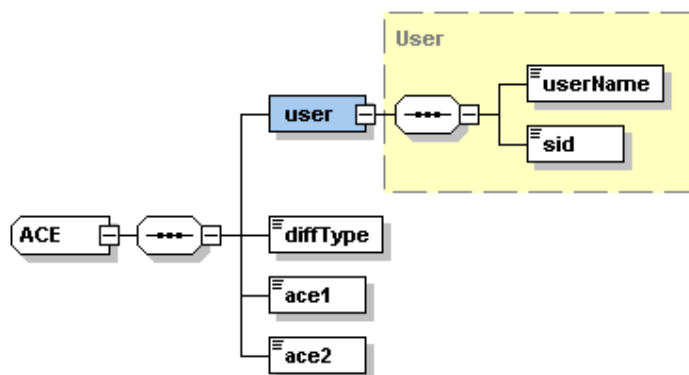
Obr. 15 Typ relace mezi type_channel a provider

4.3.1.17 type_Value



Obr. 16 Typ relace mezi type_Value a jeho vnořenými elementy

4.3.1.18 type_ACE

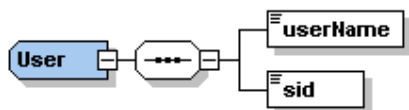


Obr. 17 Typ relace mezi type_ACE a jeho vnořenými elementy

4.3.2 Komplexní typy použity ve výstupních souborech

4.3.2.1 Typ User

Typ User se skládá z elementu userName a sid. Kde userName označuje jméno uživatele a sid je identifikátorem uživatele.

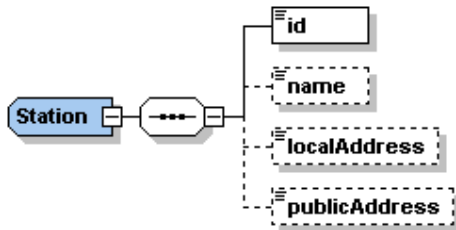


Obr. 18 Typ relace mezi typem User a jeho vnořenými elementy

4.3.2.2 Typ Station

Typ Station skládá z elementu id, name, localaddress a publicaddress.

Element <id> je identifikátorem notifikace, <name> označuje jméno stanice, <localAddress> obsahuje lokální adresu stanice a <publicAddress> veřejnou adresu stanice.

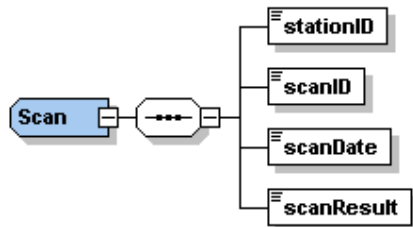


Obr. 19 Typ relace mezi typem Station a jeho vnořenými elementy

4.3.2.3 Typ Scan

Typ Scan se skládá z elementu stationID, scanID, scanDate a scanResult.

Element <stationID> je identifikátorem notifikace, <scanID> je identifikátorem scanu. <scanDate> obsahuje datum scanu a <scanResult> výsledek scanu.



Obr. 20 Typ relace mezi typem Scan a jeho vnořenými elementy

Soupis citací

[1] Microsoft Corporation: Regular Expressions as a Language [online] Dostupné na World Wide Web:

<http://msdn.microsoft.com/library/default.asp?url=/library/enus/cpguide/html/cpconregularexpressionsaslanguage.asp>

[2] W3C World Wide Web Consortium: Extensible Markup Language (XML) [online] Dostupné na World Wide Web: <http://www.w3.org/XML/>

[3] W3C World Wide Web Consortium: XML Schema [online] Dostupné na World Wide Web: <http://www.w3.org/XML/Schema>

[4] W3C World Wide Web Consortium: Cascading Style Sheets [online] Dostupné na World Wide Web: <http://www.w3.org/Style/CSS>

[5] W3C World Wide Web Consortium: Extensible HyperText Markup Language [online] Dostupné na World Wide Web: <http://www.w3.org/TR/xhtml1>

[6] Wikipedia: User Datagram Protocol [online] Dostupné na World Wide Web: http://en.wikipedia.org/wiki/User_Datagram_Protocol

Obsah

Úvod.....	1
1. Popis.....	1
2. Konfigurační soubory na straně serveru.....	2
2.1 Konfigurační soubor SysKoServer.....	2
2.1.1 Element <configuration>.....	2
2.1.2 Element <configSections>.....	3
2.1.3 Element <sysko>.....	3
2.1.4 Element <appConnectionString>.....	3
2.1.5 Element <notification>.....	4
2.1.6 Element <group>.....	4
2.1.7 Element <target>.....	4
2.1.8 Element <notify>.....	5
2.1.9 Element <checkSystem>.....	6
2.1.10 Element <checkList>.....	6
2.1.11 Element <checkItem>.....	7
2.1.12 Element <checkStation>.....	7
2.1.13 Element <checkQuery>.....	7
2.1.14 Element <excludeStation>.....	8
2.1.15 Element <accessRights>.....	8
2.1.16 Element <stationGroup>.....	8
2.1.17 Element <station>.....	9
2.1.18 Element <process>.....	9
2.1.19 Element <allowGroup>.....	9
2.1.20 Element <wak.wnt.remoting>.....	10

2.1.21	Element <channel>.....	10
2.2	Konfigurační soubory na straně klienta.....	10
2.2.1	Konfigurační soubor SysKoConsole	10
2.2.2	Element <configuration>.....	11
2.2.3	Element <configSections>	11
2.2.4	Element <sysko>	12
2.2.5	Element <appSettings>	12
2.2.6	Element <scanner>	12
2.2.7	Element <scan>	12
2.2.8	Element <fileSystem>	13
2.2.9	Element <registry>	13
2.2.10	Element <services>	14
2.2.11	Element <shares>	14
2.2.12	Element <policy>	14
2.2.13	Element <eventLog>	15
2.2.14	Element <events>	15
2.2.15	Element <log>	15
2.3	Konfigurační soubor SysKoApp	16
3.	Výstupní soubory.....	17
3.1	scanDiff	17
3.1.1	Element <scanDiffList>	18
3.1.2	Element <scanDiff>	18
3.1.3	Element <station>	18
3.1.4	Element <scan1>	18
3.1.5	Element <scan2>	19
3.1.6	Element <name>	19
3.1.7	Element <type>	20

3.1.8	Element <Values>.....	20
3.1.9	Element <ACEs>.....	20
3.2	EventLog	21
3.2.1	Hierarchie elementů	21
3.2.2	Element <EventLog>	21
3.2.3	Element <event>	21
3.2.4	Element <user>	22
3.2.5	Element <stationID>	22
3.2.6	Element <logName>.....	22
3.2.7	Element <machineName>	23
3.2.8	Element <eventDate>.....	23
3.2.9	Element <eventID>	23
3.2.10	Element <eventType>	23
3.2.11	Element <eventSource>	24
3.2.12	Element <eventDescription>.....	24
3.3	scanList.....	24
3.3.1	Hierarchie elementů	24
3.3.2	Element <scanList>.....	25
3.3.3	Element <scan>	25
3.3.4	Element <stationID>	25
3.3.5	Element <scanID>.....	25
3.3.6	Element <scanDate>.....	26
3.3.7	Element <scanResult>.....	26
3.4	Stations	26
3.4.1	Element <Stations>	26
3.4.2	Element <station>	27
3.4.3	Element <id>	27

3.4.4	Element <name>	27
3.4.5	Element <localAddress>	28
3.4.6	Element <publicAddress>	28
3.5	CheckSystemList	28
3.5.1	Element <CheckSystemList>	29
3.5.2	Element <CheckSystem>	29
3.5.3	Element <scan>	30
3.5.4	Element <checkRequestItem>	30
3.5.5	Element <name>	30
3.5.6	Element <type>	30
3.5.7	Element <currentValue>	31
3.5.8	Element <op>	31
3.5.9	Element <reqValue>	31
3.5.10	Element <result>	31
4.	Seznam typů a struktur	32
4.1	Základní datové typy	32
4.2	Jednoduché odvozené typy	32
4.2.1	Jednoduché typy použité v konfiguračních souborech	32
4.3	Komplexní typy	34
4.3.1	Komplexní typy použité v konfiguračních souborech	34
4.3.2	Komplexní typy použity ve výstupních souborech	36
	Soupis citací	39

Slovníky

Zkratky

Zkratka	Význam
OS	Operační systém

Tab. 4 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.
XML schéma	XML schéma popisuje strukturu XML dokumentu.
CSS	Cascading Style Sheet. Technologie pro přidávání stylu k webovým dokumentům.
XHTML	Extensible HyperText Markup Language. Značkovací jazyk.
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 uvozující a ukončující řetězcem "@@". Po vyhodnocení systémem je jeho hodnota nahrazena významem makra. Např. hodnotou makra @@WINDIR@@ může být řetězec "C:\WINNT".
UDP	User Datagram Protocol
ACE	Access Control Entry. Obsahuje množinu přístupových práv a bezpečnostní identifikátor, který identifikuje uživatele pro kterého jsou práva povolena, zakázána a auditována.

Tab. 5 Slovník termínů

