IBM Systems and Technology Group

RACF SMF Unload and XML

Walt Farrell, CISSP
IBM Corporation
wfarrell@us.ibm.com
May, 2007

ON DEMAND BUSINESS™

Disclaimer

- The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.
- In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.
- It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.
- IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.
- **References to non-IBM products are not intended as recommendations, merely as examples of some of the products that are available**

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - OS/390
  - z/OS
  - RACF
- Apache is a trademark of The Apache Software Foundation.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Other company, product, or service names may be trademarks or service marks of others.

Agenda

- **Acknowledgements**
- **XML is…**
- **SMF Unload enhancements for V1R7**
- **Quick Intro to XML**
  - File types of interest
  - simple.xml document
  - simple.xsd document
  - Validating the simple.xml document using simple.xsd
- **securityEventLog**
- **Applications**
  - ISPF
  - Web browser
  - XSLT
  - DB2 v9
  - Other reporting packages
- **Where to get more info**
- **Summary**

Acknowledgements

- **This presentation is heavily based on one originally created by my colleague Peggy LaBelle**
- **The IBM DeveloperWorks web site provided a wealth of useful information for my research**

XML is…

- **XML – eXtensible Markup Language**
- **W3C standard for document markup**
  - Script, Bookmaster, Foils, html
- **A metamarkup language**
  - The language is highly customizable
  - Create your own tag names
  - Create your own grammar
- **Looks like HTML however**
  - XML focuses on describing the data not how the data should look
  - Stricter in enforcing syntax
- **Used for**
  - Document interchange
  - Rendering data into different formats

HTML Example

```
<html>
<body>
<p><b>Event Type</b>
<p>JOBINIT
```

Would display:

Event Type
JOBINIT

HTML Example

```
<html>
<body>
<p><b>These are a Few of <br>
My Favorite Events</b>
<p>JOBINIT
```

Would display:

These are a Few of
My Favorite Events
JOBINIT

Simple XML Instance Document

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
<simpleEventLog xmlns='http://www.ibm.com/Simple'>
  <!-- a simple event -->
  <event>
    <eventType>JOBINIT</eventType>
  </event>
</simpleEventLog>
```

Processing Instructions	<?...?>
Elements	<name>…</name> or <name/>
Comments	<!-- … -->
Attributes	type='…' or type="…"
Namespaces	xmlns='name' or xmlns:prefix='name'
File	simple.xml

z/OS V1R7 Security Server RACF
z/OS V1R7 Integrated Security Services EIM

- **SMF Unload option to create XML documents from raw SMF records**
- **securityEventLog XML tags and grammar documented in schema document**
  - Caution: imprecise
  - IRRSCHEM
  - IRREIMSC
- **Provides a new basis for creating new kinds of audit reports**

Some file types associated with XML

- xxx.xml **- XML document**
- xxx.xsd **- XML Schema document**
- xxx.dtd **- Document type definitions (old style schema documents)**
- xxx.xsl **- Extensible Style Sheet Language document**
- **Predecessors to XML and XSLT**
  - **xxx.html** - Hyper-text markup language
  - **xxx.css** - Cascading Style Sheets

XML software components

- Parsers **are syntax checkers for XML documents**
  - Check xml documents for **well-formedness**
  - Optional validation of elements using schema documents
  - Examples:
    - Standards for parsers - **DOM** (W3C) and **SAX** (defacto)
    - Apache Software Foundation (www.apache.org) implementations
      - **Xerces** (from Xerces Blue butterfly)
      - Java, C/C++, Perl wrapper around the C/C++, COM wrapper
    - **XML Toolkit for z/OS** (C/C++ or Java)
- Processors **are one kind of XML applications**
  - Examples
    - Apache Software Foundation Implements
      - **Xalan**
      - Java
    - XML Toolkit for z/OS has an XSLT processor (C/C++ or Java)

Simple XML Instance Document

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
<simpleEventLog xmlns='http://www.ibm.com/Simple'>
  <!-- a simple event -->
  <event>
    <eventType>JOBINIT</eventType>
  </event>
</simpleEventLog>
```

Processing Instructions	<?...?>
Elements	<name>…</name> or <name/>
Comments	<!-- … -->
Attributes	type='…' or type="…"
Namespaces	xmlns='name' or xmlns:prefix='name'
File	simple.xml

Simple Schema Document

```
<?xml version="1.0"?>
<xs:schema targetNamespace="http://www.ibm.com/Simple"
    elementFormDefault="qualified" attributeFormDefault="unqualified"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="http://www.ibm.com/Simple">
  <xs:element name="simpleEventLog">
    <xs:complexType>
      <xs:sequence>
      <xs:element name="event" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
          <xs:element name="eventType"   type="xs:string"    />
          </xs:sequence>
        </xs:complexType>
      </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

- A schema document is an XML document
- Defines tag names
- Validating parsers compare XML doc to schema definition
- simple.xsd

Validating an Instance Document

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
<simpleEventLog xmlns='http://www.ibm.com/Simple'
   xmlns:xsi='http://www.w3.org/2001/XMLSchema-instance'
   xsi:schemaLocation='http://www.ibm.com/Simple/Simple.xsd'>
  <!-- a simple event -->
  <event>
    <eventType>JOBINIT</eventType>
  </event>
</simpleEventLog>
```

1. Add a mapping of namespace to schema document
2. Make sure schema document accessible to parser
3. Run xml document through the validating parser

java sax.Counter –v –s –f simple.xml

This can be done on USS or Windows. Requires Java and XML parser

The securityEventLog

- **XML instance document created by SMF Unload**
  - Tabular format still supported
- **Two kinds of documents - unformatted and formatted**
- **All events are supported (30, 80, 81, and 83)**
- **Tag for each field in an event**
  - Tag name derived from the corresponding DB2 field name
- **Schema defined in**
  - IRRSCHEM and IRREIMSC in SYS1.SAMPLIB
  - Schema documents are ASIS Code

securityEventLog XML Tag Language

- **Tag names are derived from the DB2 field names (exceptions are documented). Camel back notation.**
  - Example:

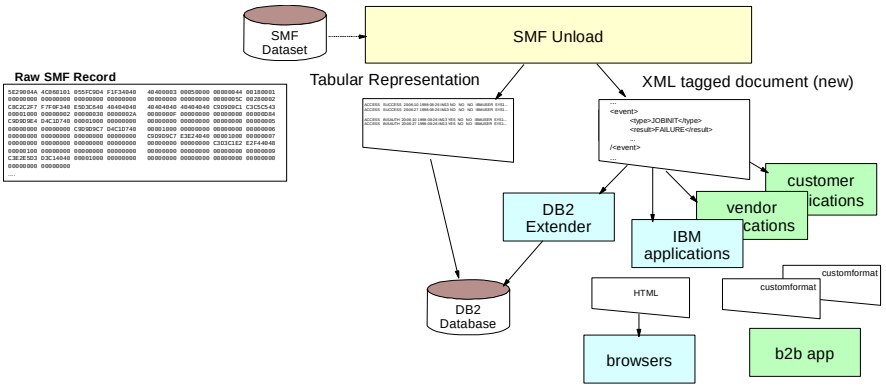
    RINI_TIME_WRITTEN becomes
    <timeWritten>…</timeWritten>

- **XML document may contain more data than tabular output**
  - <col>_TIME_WRITTEN is to 1/10ths
  - timeWritten is to 1/100ths for Type 83, subtype 2 and above events

  Note: Partially addresses marketing requirement MR0714032340
  - Tabular has a truncation indicator after the field

SMF Unload in z/OS V1R7

- **XML support added**
- **EIM events supported**



SMF Unload - Job

```
//SMFUNLD JOB ,'SMF DATA UNLOAD',
// MSGLEVEL=(1,1)
//SMFDUMP EXEC PGM=IFASMFDP
//SYSPRINT DD SYSOUT=A
//ADUPRINT DD SYSOUT=A
//OUTDD DD DISP=SHR,DSN=USER01.RACF.IRRADU00
//SMFDATA DD DISP=SHR,DSN=USER01.RACF.SMFDATA
//SYSIN DD *
  INDD(SMFDATA,OPTIONS(DUMP))
  OUTDD(SMFOUT,TYPE(000:255))
  ABEND(NORETRY)
  USER2(IRRADU00)
  USER3(IRRADU86)
/*
```

- **Control the output**
  - OUTDD DD - tabular output
  - XMLOUT DD - unformatted XML document
  - XMLFORM DD - formatted XML document

SMF Unload Output

Tabular

```
ADDUSER  SUCCESS  21:51:55 2005-01-17 IM13 NO   NO   NO   IBMUSER  SYS1 …
ALTUSER  SUCCESS  21:51:59 2005-01-17 IM13 NO   NO   NO   IBMUSER  SYS1 …
```

XML Document - Part 1

```
<?xml version='1.0' encoding='ebcdic-cp-us' ?>
<securityEventLog xmlns='http://www.ibm.com/xmlns/zOS/IRRSchema'>

  <rdf:Description rdf:about=''
              xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#'
              xmlns:dc='http://purl.org/dc/elements/1.1/'>
   <dc:creator>z/OS Security Server RACF SMF Unload (HRF7720)</dc:creator>
   <dc:subject>RACF Security Event Log 2005-01-17 22:12:09</dc:subject>
   <dc:language>en</dc:language>
  </rdf:Description>
  …Events…
</securityEventLog>
```

SMF Unload - Output

- XML Unformatted (XMLOUT DD)

```
<event><eventType>ADDUSER</eventType><eventQual>SU…… </event>
```

- XML Formatted (XMLFORM DD)

```
<event>
  <eventType>ADDUSER</eventType>
  <eventQual>SUCCESS</eventQual>
  <timeWritten>21:51:55.54</timeWritten>
  <dateWritten>2005-01-17</dateWritten>
  <systemSmfid>IM13</systemSmfid>
  <prodFmid>HRF7720</prodFmid>
  <prodName>RACF</prodName>
  <details>
    <violation>N</violation>
  …
</event>
```


A JOBINIT Style Sheet

```
<?xml version="1.0"?>
<xslt:transform version="1.0"
xmlns:xslt="http://www.w3.org/1999/XSL/Transform">
 <xslt:output method="html"/>

 <xslt:template
   match="securityEventLog">
  <HTML>
   <BODY>
    <DIV STYLE="font-family:Verdana;">
     <H1>RACF Event Log Report</H1>
      <xslt:apply-templates/><BR/>
    </DIV>
   </BODY>
  </HTML>
 </xslt:template>
```

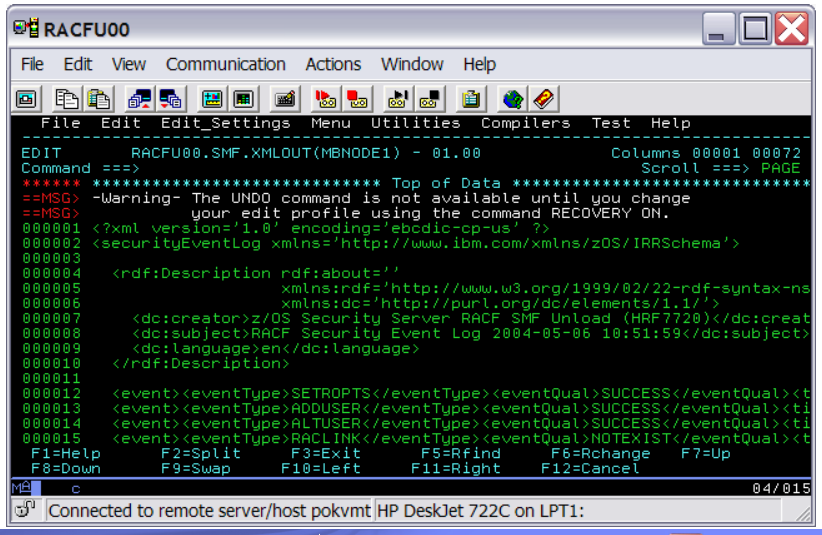
```
<xslt:template
   match="event[eventType='JOBINIT']">
   <P><xslt:value-of select="position()"/>:
   Event/<xslt:value-of select="eventType"/>
   Qual/<xslt:value-of select="eventQual"/>
   Date/<xslt:value-of select="dateWritten"/>
   Time/<xslt:value-of select="timeWritten"/>
   </P>
 </xslt:template>

 <!-- ignore unmatched nodes -->
<xslt:template match="text()">
</xslt:template>
</xslt:transform>
```

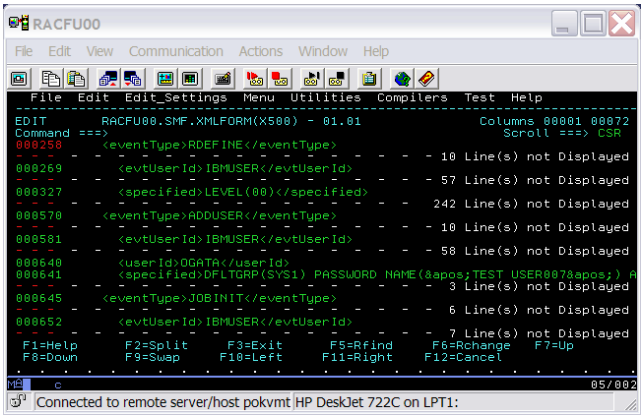
Application Examples

- **ISPF**
- **Web browser**
- **XSLT**
- **DB2**
- **Other reporting packages**

ISPF - XMLOUT Format



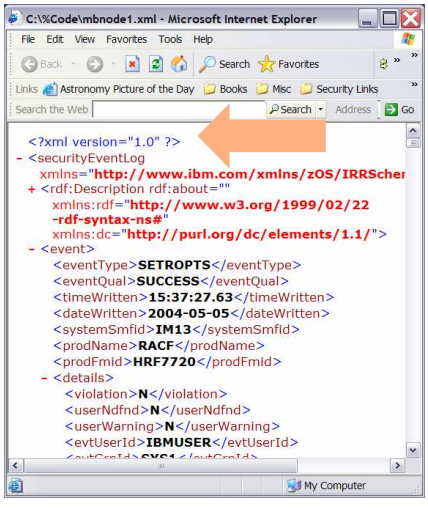
ISPF - XMLFORM + ISPF Commands



ISPF commands:
exclude all
find <eventType>
find <evtUserId> or
find <evtUserId>R00
find <specified> all

However: Editing can require a very large region!
Browse is more likely. Still, browsing XML may be easier than tabular

Browsing an XML document



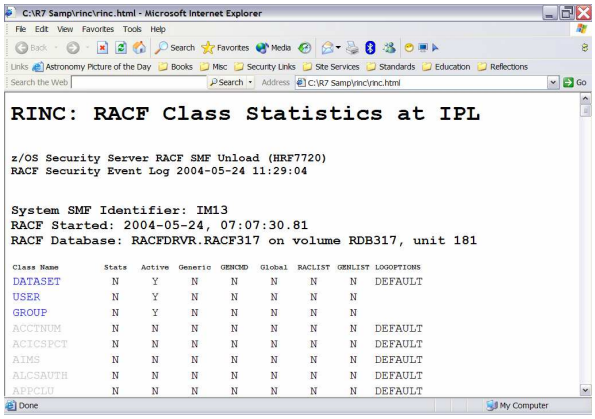
- Download must convert to ASCII
- Delete **encoding='ebcdic-cp-us'**

Firefox and Internet Explorer both support displaying “raw” XML, and you can collapse sections using the + and -

More Ideas for Web Browsing

- **Pre-build XSLT stylesheets, or CSS (cascading style sheets)**
- **Pre-process the XML with REXX, or DFSORT/ICETOOL, etc. to remove the encoding specification and add the XSL/CSS specifications.**
- **You can reference more than one XSL or CSS style**
  - E.g., have one that shows ACCESS events, another that shows JOBINIT events. Or one that shows SUCCESSes, one that shows FAILUREs
  - Firefox user can choose the report he wants, via View->Page Style

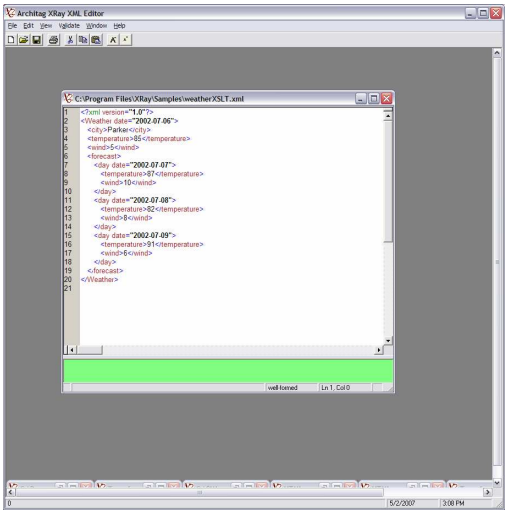
Using an XSLT style sheet



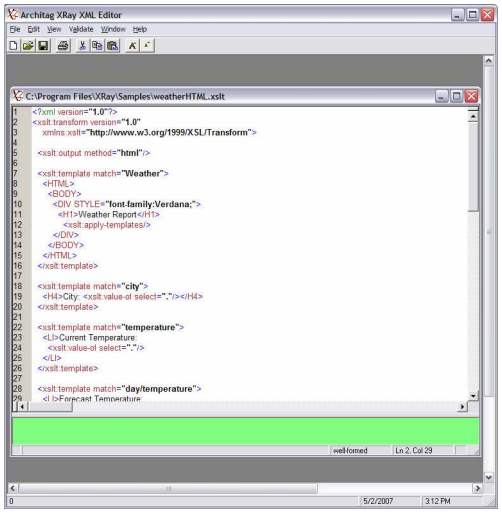
Using an XSLT Style Sheet

- **Design the style sheet**
- **Generate html using an XSLT processor**
  - Input: xxx.xml, yyy.xslt
  - Output: zzz.html
- **Ex. java org.apache.xalan.xslt.Process -in ..\pwrule.xml -xsl rinc.xsl -out rinc.html**
- **Can download Xalan from Apache.org for use on PC, or download the XML Toolkit for z/OS and run it on z/OS**

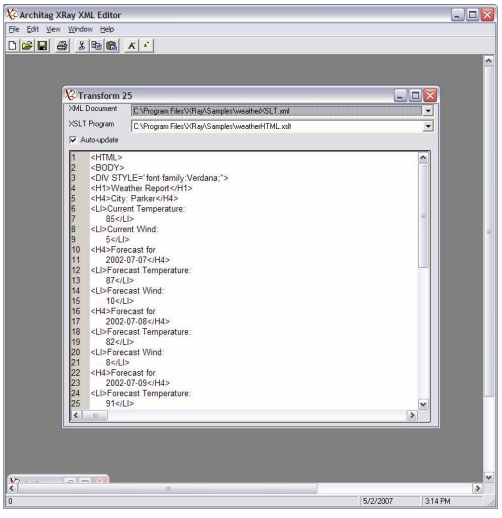
Architag XRay XML Editor (XML file)



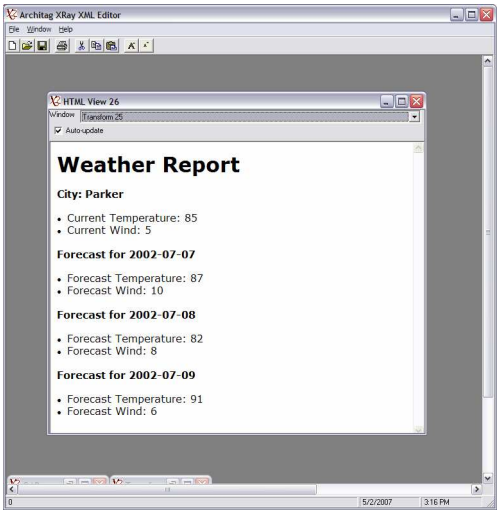
Architag XRay XML Editor (XSLT file)



Architag XRay XML Editor (Applying the Transform)



Architag XRay XML Editor (Viewing the HTML)



Using DB2 with XML

- DB2 before v9 needs DB2 extender product to work with DB2
- DB2 v9 supports XML natively.
  - Define tables with XML columns
  - Each table row contains complete XML document
    - Each row might be one day's set of records, or one SMF Unload
  - Can use XQuery and XPath statements to perform queries and generate reports
- You can download a free copy of DB2 v9 (with XML support) for your PC at http://www-306.ibm.com/software/data/db2/express/

Other Reporting Packages

- Pentaho (formerly JFreeReport) is a free, open-source product that generates reports and PDF from:
  - SQL databases; should work with DB2 v9.
  - XML files directly
  - Has a Report Design Wizard and a more complete (but harder to use) Report Designer
  - Also supports integration into other programs
  - http://www.pentaho.com
- JasperReports is another free, open-source product that generates reports, PDF, XML, etc. from SQL databases and XML
  - Has a report design wizard (iReport)
  - Also supports integration into other programs
  - http://www.jasperforge.org

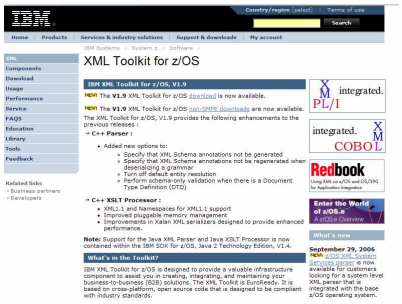
Other ideas

- **Convert securityEventLog to**
  - A different XML tag language
  - To text
  - To a new tabular format
  - Add graphics
  - Pie charts
- **Cautions:**
  - Amount of data that can be processed is a concern, especially on PC; Consider experimenting on PC but doing production on host

Where to Get Information

- **Formal IBM Classes in XML that Peggy found helpful**
  - XM301 Introduction to XML and Related Technologies (2.5 days)
  - XM321 Programming XML and Related Technologies for Java (2.5 days)
  - http://www.ibm.com/training
- **IBM Developer Works has a section on XML including "New to XML"**
  - Many **free** tutorials on XML, XSLT, Xpath, Xquery. Some I've taken:
    - Intro to XML
    - Intro to XSLT
    - Using CSS to process XML
    - Processing XML using Xquery
  - http://www.ibm.com/developerworks/xml

XML Parsers and Processors



- IBM XML Toolkit for z/OS
  http://www.ibm.com/servers/eserver/zseries/software/xml/
- Apache Software Foundation
  http://www.apache.org/

Summary

- securityEventLog XML documents are…
  - Readable!
  - Flexible and extendable
  - Contains more data
  - Enables data interchange
  - Transformation between formats…XML Document + Style Sheet => web pages, filtered data, pie charts, …
  - Displayable on a browser