OVAL Tutorial

Jon Baker

July 12th, 2006

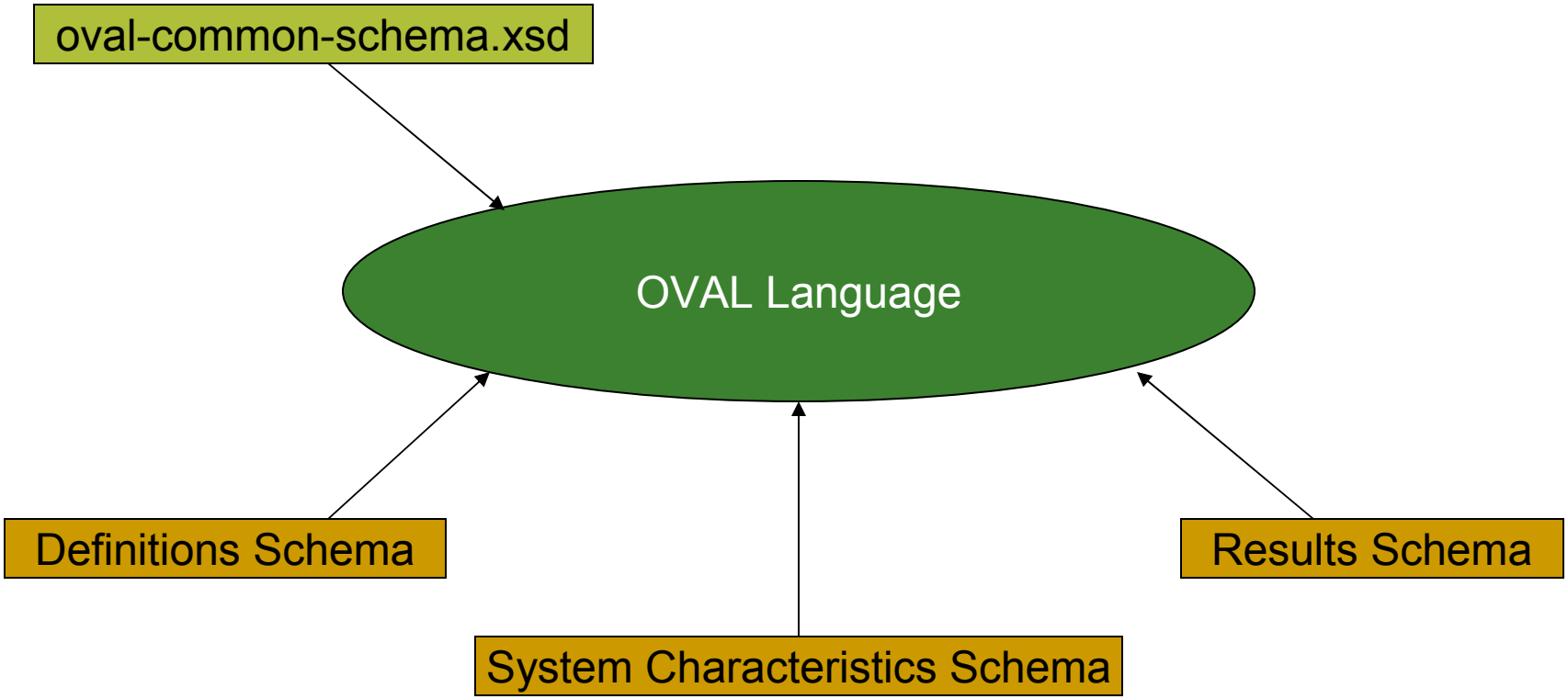
Agenda

- Welcome to OVAL 5!
- How are the schemas related?
- OVAL Definition Tutorial
  - The basics
    - Definition structure
    - Hello World
    - OVAL Definitions document
  - Advanced topics
    - Extended Definitions
    - Variables
    - Complex objects
    - Behaviors
    - Nil
- Questions and more info…

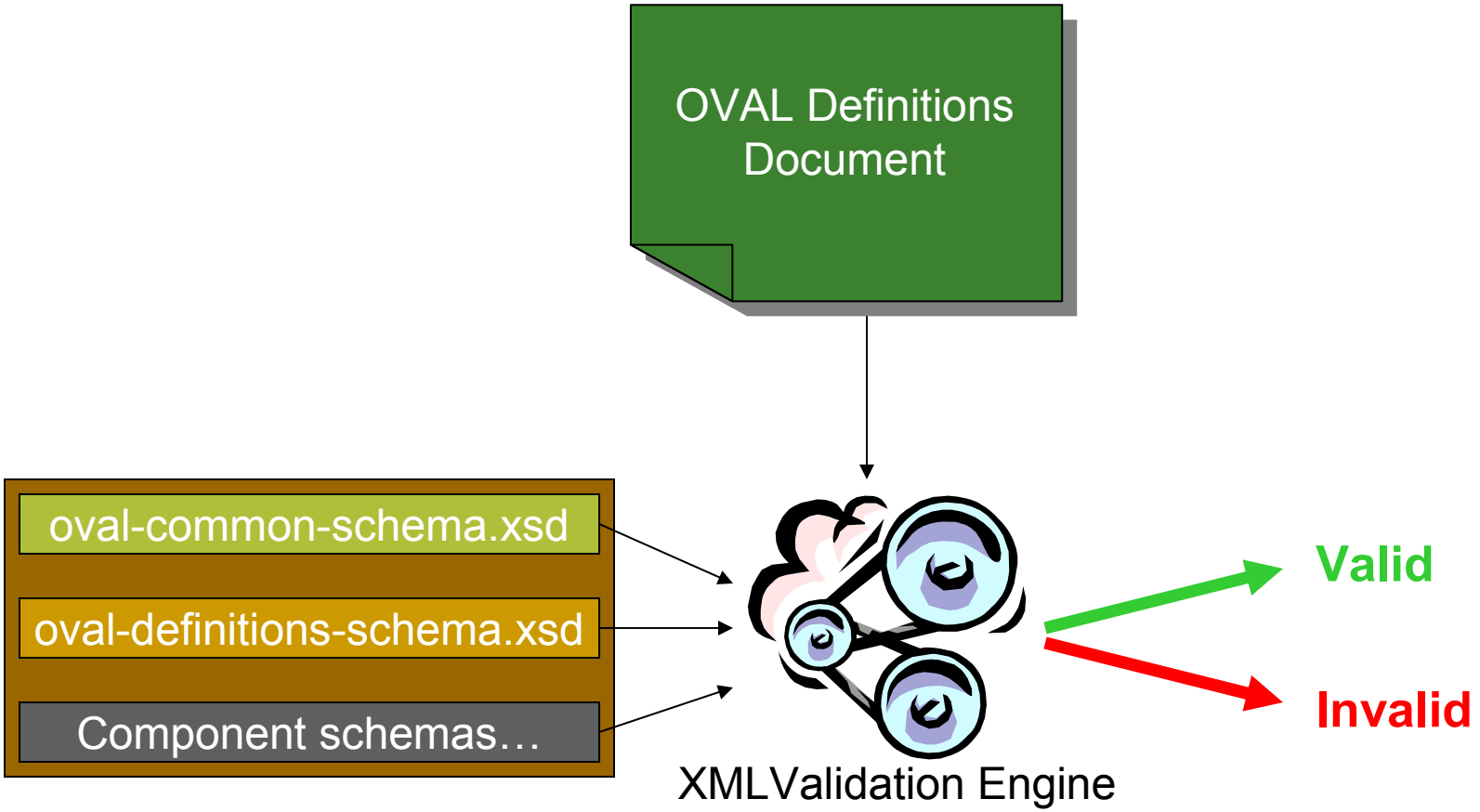
Welcome to OVAL 5!

- New OVAL Id formats
- Creation of a Common Schema
- Definition Schema
  - Extended definitions
  - Enhanced system object specification.
  - Redesigned variable format
  - Common Linux schema
  - Enhanced definition metadata
  - New component schemas and additions to existing components schemas
- Redesigned Results Schema
- Restructure System Characteristics Schema
- Schematron validation

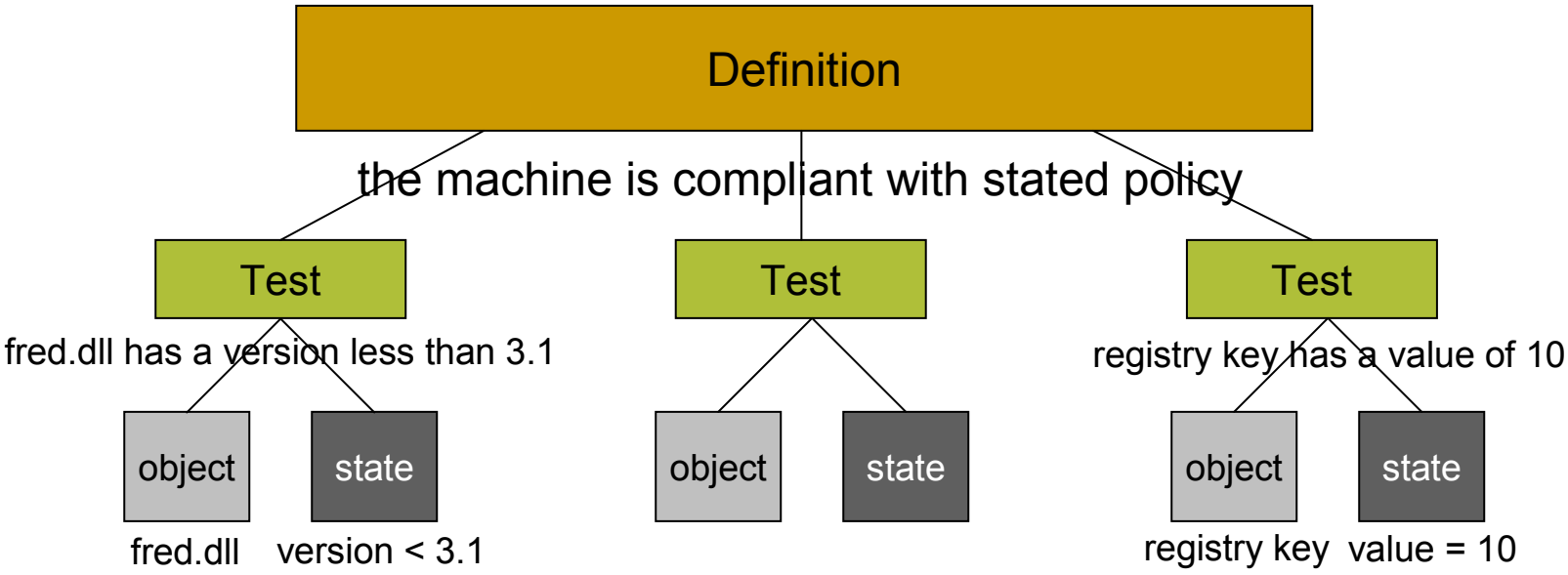
How are the schemas related? OVAL Language



How are the schemas related? Definition Schema

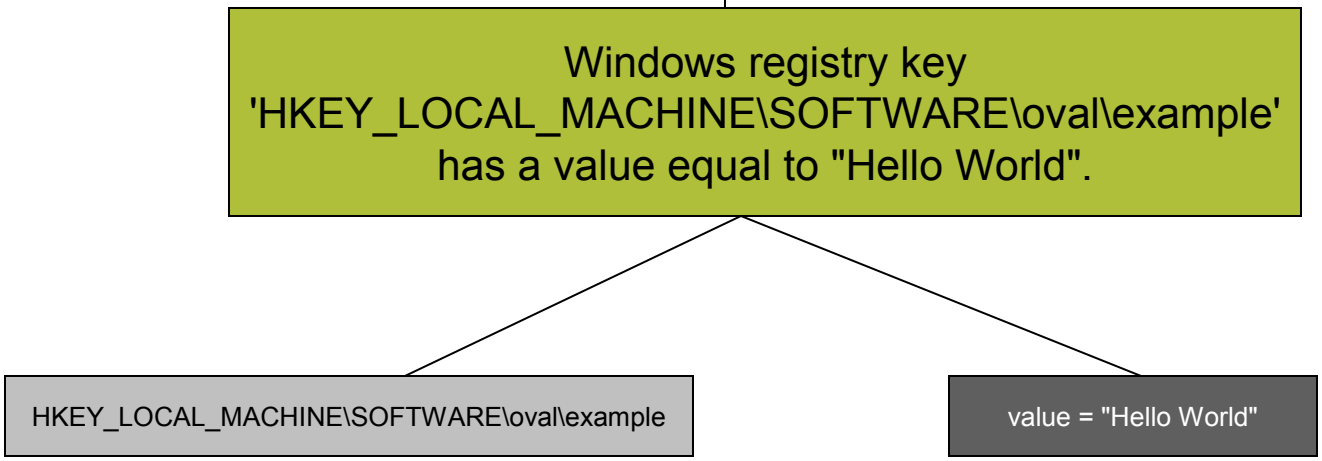


OVAL Definition Tutorial - definition structure

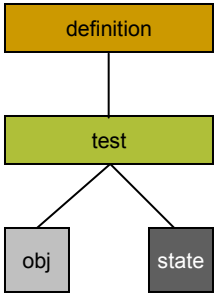


Hello World

write an OVAL Definition to test that the (hypothetical) Windows registry key 'HKEY_LOCAL_MACHINE\SOFTWARE\oval\example' has a value equal to "Hello World".

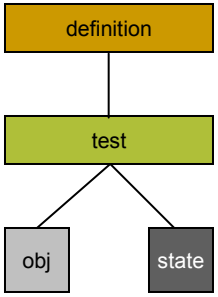


Hello World - Registry Object



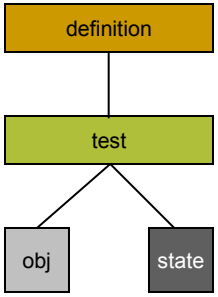

```
<registry_object id="oval:org.mitre.oval.tutorial:obj:1">
    <hive>HKEY_LOCAL_MACHINE</hive>
    <key>SOFTWARE\oval</key>
    <name>example</name>

</registry_object>
```

Hello World - Registry State



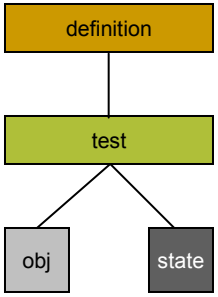

```
<registry_state id="oval:org.mitre.oval.tutorial:ste:1">
    <value operation="equals">Hello World</value>
</registry_state>
```

Hello World - Registry Test




```
<registry_test id="oval:org.mitre.oval.tutorial:tst:1" check="all">
    <object object_ref="oval:org.mitre.oval.tutorial:obj:1"/>
    <state state_ref="oval:org.mitre.oval.tutorial:ste:1"/>
</registry_test>
```

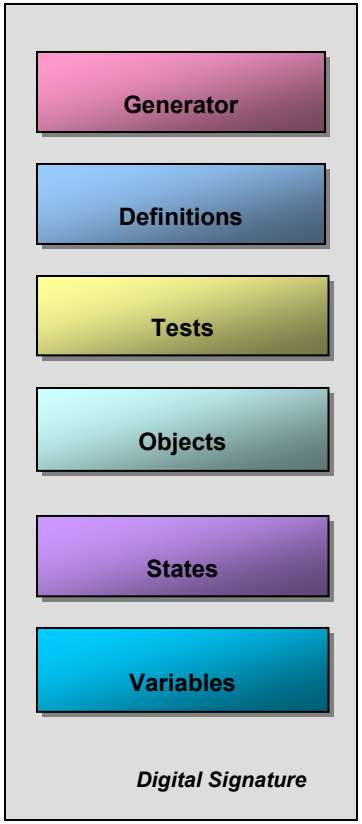
Hello World - OVAL Definition




```
<definition id="oval:org.mitre.oval:obj:1">
    <metadata>
        <title>Hello World Example</title>
        <description>
            This definition is used to introduce the OVAL Language
            to individuals interested in writing OVAL Content.
        </description>
    </metadata>
    <criteria>
        <criterion test_ref="oval:org.mitre.oval.tutorial:tst:1"
    comment="the value of the registry key equals Hello World"/>
    </criteria>
</definition>
```

OVAL Definitions Document

- Generator
- Definitions
- Tests
- Objects
- States
- Variables
- Digital Signature



OVAL Definitions Document - Namespaces

- namespace vs prefix
  - xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
- default namespace
  - xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
- How OVAL uses namespaces
  - <oval:schema_version>5.0</oval:schema_version>
  - <file_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#**windows**">
  - <file_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#**unix**">

OVAL Definitions Document - SchemaLocation

- used to identify schema file(s) for validation

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
        xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
        xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
        xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd
                http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd
                http://oval.mitre.org/XMLSchema/oval-definitions-5#windows windows-definitions-
    schema.xsd">

    <definitions> ... </definitions>

</oval_definitions>
```

Which schema file is used to validate the <definitions> element?

OVAL Definitions Document - Generator Section

- Information about how the OVAL Document was created
  - product name
  - product version
  - schema version
  - timestamp
- Not about the content, but about the document!

```
<generator>
        <oval:product_name>Guide Writer</oval:product_name>
        <oval:product_version>1.2</oval:product_version>
        <oval:schema_version>5.0</oval:schema_version>
        <oval:timestamp>2005-10-12T18:13:45</oval:timestamp>
</generator>
```

OVAL ID Format

- Globally unique urn
  - oval : org.mitre.oval : def : 123
- 4 components
  1. oval - prefix
  2. org.mitre.oval – reverse dns style namespace
  3. def - id type (def, tst, ste, obj, var)
  4. 123 - unique integer

OVAL Definitions Document - Digital signature

- Defined by the XML-Signature Syntax and Processing W3C Recommendation
- Enveloped Signature - The signature is over the XML content that contains the signature as an element.

Advanced Topics

Extended Definitions

- Existing definitions may be extended.
  - Add workarounds to an existing vulnerability def
- Common units of logic can be broken out.
  - Microsoft Windows XP SP2 is installed
- Easier/Faster to create new definitions

Variables

- Define values to be obtained at run time.
- Represent an array of values
- Three types
  - local_variable
  - external_variable
  - constant_variable

Variables - constant_variable

- Value is set by definition author.
- helpful when
  - creating complex variables.
  - easy reuse of common constant values

```
<constant_variable comment="…" datatype="string" version="1" id="…">
   <value>system32</value>
</constant_variable>
```

Variables - local_variable

- Value determined at definition analysis time.
- Manipulate values fetched from objects, other variables, or literals.
- Functions (concat, substring, split, …)

```
<constant_variable datatype="string" id="var1">
   <value>\system32</value>
</constant_variable>
<local_variable id="var2" datatype="string">
   <concat>
      <object_component item_field="value" object_ref="obj1"/>
      <variable_component var_ref="var1"/>
   </concat>
</local_variable>
```

Variables - external_variable

- Defines a variable with an external source.
- Gives suggestion about type of data and reasonable values.

```
<external_variable comment="in the range 8-16, or 32" datatype="int " id="var1">
   <possible>
      <restriction hint="min allowed is 8" operation="greater than">7</restriction>
      <restriction hint="max allowed is 16" operation="less than">17</restriction>
   </possible>
   <possible>
      <possible>32</possible>
    </possible>
</external_variable>
```

Complex Objects - intro

An Object in OVAL 5 identifies 0 or more items on a system.

Set consists of all registry keys that match the object

```
<registry_object …>
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>ExampleKey</key>
   <name>ExampleName</name>
</registry_object>
```

```
<registry_object …>
   <hive>HKEY_LOCAL_MACHINE</hive>
   <key>ExampleKey</key>
   <name operation="pattern match">.*</name>
</registry_object>
```

Complex Objects - set element

- OVAL 5 adds ability to manipulate these sets.
  - set element
    - set_operator
    - object references
    - filters

Set consists of all registry keys that match the criteria

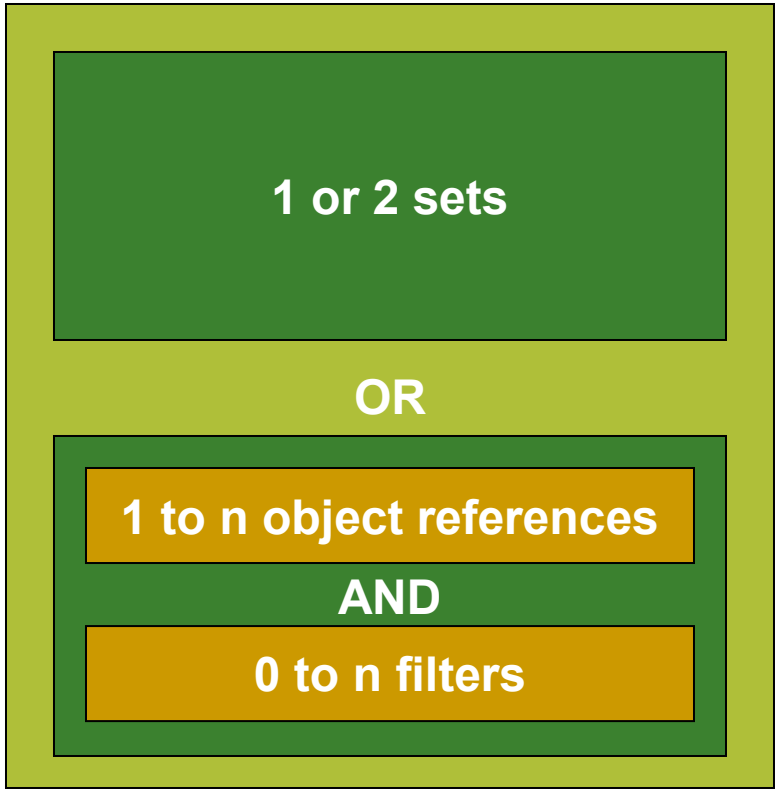
```
<registry_object …>
   <set set_operator="UNION">
      <object_reference>objId1</object_reference>
      <object_reference>objId2</object_reference>
      <filter>stateId1</filter>
      <filter>stateId2</filter>
   </set>
</registry_object>
```

Complex Objects - set element - details

- Element contents
  - 1 or 2 child set element

  OR
  - 1 to n object_reference elements

    and
  - 0 to n filters
- set_operator attribute
  - UNION
  - COMPLEMENT
  - INTERSECTION



Complex Objects - Filters

- A filter is a state that is used to "filter out" items from a set.
- Any number of filters can be applied.
- Filters are applied before the set_operator is applied.

Complex Objects

Trustees not part of the ADMINISTRATORS group or the user SYSTEM do not have access to the specified file.

- Identify the file.
- Identify the trustees that should not have access.
  - Identify all trustees on the system
  - and remove the trustees in the admin group
  - and remove the System user
- Check permissions on the file for each trustee that should not have access.

Behaviors

- Allow more detailed definition of an Object
- Implemented on a per object basis
- Guides data collectors
- file_object example:
  - Behaviors defined for a file_object
    - max_depth – controls how deep to search
    - recurse_direction – controls direction of search

Nil vs. pattern match .*

Confirm that the specified directory exists…

- Nil allows authors to specify higher level objects.
- Nil is only allowed on select entities.
- Implemented with xsi:nil="true"
- file_object example:
  - xsi:nil="true" on filename entity
    - Don't collect file information.
  - Pattern match .* on filename entity
    - Collect file information about all files.

Questions and more info…

- http://oval.mitre.org/language
- Posting improved samples & better documentation.

- ???

Back up slides

Hello World - Full XML

```
<oval_definitions …>
  <generator>…</generator>
  <definitions>
    <definition id="oval:org.mitre.oval.tutorial:def:1" version="1" class="miscellaneous">
      <metadata>
        <title>Hello World Example</title>
        <affected family="windows"/>
        <description>This definition is used to introduce the OVAL Language to individuals interested in writing OVAL Content.</description>
      </metadata>
      <criteria comment="Software section" operator="AND">
        <criterion comment="The oval example registry key has a value of &amp;quot;Hello World&amp;quot;" test_ref="oval:org.mitre.oval.tutorial:tst:1"/>
      </criteria>
    </definition>
  </definitions>
  <tests>
    <registry_test id="oval:org.mitre.oval.tutorial:tst:1" version="1" check="at least one" comment="The oval example registry key has a value of &amp;quot;Hello
        World&amp;quot;" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
      <object object_ref="oval:org.mitre.oval.tutorial:obj:1"/>
      <state state_ref="oval:org.mitre.oval.tutorial:ste:1"/>
    </registry_test>
  </tests>
  <objects>
    <registry_object id="oval:org.mitre.oval.tutorial:obj:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
      <hive>HKEY_LOCAL_MACHINE</hive>
      <key operation="equals">SOFTWARE\oval</key>
      <name operation="equals">example</name>
    </registry_object>
  </objects>
  <states>
    <registry_state id="oval:org.mitre.oval.tutorial:ste:1" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
      <value operation="equals">Hello World</value>
    </registry_state>
  </states>
</oval_definitions>
```

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
                  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
                  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
                  xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
                  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd
                                      http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd
                                      http://oval.mitre.org/XMLSchema/oval-definitions-5#windows windows-definitions-schema.xsd">

      <generator>
            <oval:schema_version>5.0</oval:schema_version>
            <oval:timestamp>2005-10-12T18:13:45</oval:timestamp>
      </generator>

      <definitions>
            <definition id="oval:org.mitre.oval:def:999" version="1" class="inventory">
                  <metadata>
                        <title>Microsoft Windows Server 2003 32-Bit Edition is installed</title>
                        <affected family="windows">
                              <platform>Microsoft Windows Server 2003</platform>
                        </affected>
                        <description>A version of Microsoft Windows Server 2003 32-Bit Edition is installed.</description>
                  </metadata>
                  <criteria operator="AND">
                        <criterion test_ref="oval:org.mitre.oval:tst:61" comment="Windows Server 2003 is installed"/>
                        <criterion test_ref="oval:org.mitre.oval:tst:72" comment="32-Bit version of Windows is installed"/>
                  </criteria>
            </definition>
      </definitions>

      ...
```

Example

```
...

<tests>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~   windows registry tests   ~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <registry_test id="oval:org.mitre.oval:tst:61"
                     version="1"
                     check="at least one"
                     comment="Windows Server 2003 is installed"
                     xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <object object_ref="oval:org.mitre.oval:obj:3"/>
            <state state_ref="oval:org.mitre.oval:ste:3"/>
      </registry_test>
      <registry_test id="oval:org.mitre.oval:tst:72"
                     version="1"
                     check="at least one"
                     comment="32-Bit version of Windows is installed"
                     xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <object object_ref="oval:org.mitre.oval:obj:4"/>
            <state state_ref="oval:org.mitre.oval:ste:4"/>
      </registry_test>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
</tests>

...
```

Example

```
...
<objects>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~   windows registry objects   ~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <registry_object id="oval:org.mitre.oval:obj:3" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <hive>HKEY_LOCAL_MACHINE</hive>
            <key>SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
            <name>CurrentVersion</name>
      </registry_object>
      <registry_object id="oval:org.mitre.oval:obj:4" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <hive>HKEY_LOCAL_MACHINE</hive>
            <key>SYSTEM\CurrentControlSet\Control\Session Manager\Environment</key>
            <name>PROCESSOR_ARCHITECTURE</name>
      </registry_object>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
</objects>
<states>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~   windows registry states   ~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <registry_state id="oval:org.mitre.oval:ste:3" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <value>5.2</value>
      </registry_state>
      <registry_state id="oval:org.mitre.oval:ste:4" version="1" xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
            <value>x86</value>
      </registry_state>
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
      <!-- ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ -->
</states>
...
```

Example

```
      ...

      <variables>
            <local_variable id="oval:org.mitre.oval:var:1" version="1" datatype="string" comment="Windows system32 directory">
                  <concat>
                        <object_component object_ref="oval:org.mitre.oval:obj:123" item_field="value"/>
                        <literal_component>\system32\</literal_component>
                  </concat>
            </local_variable>
      </variables>

</oval_definitions>
```