@variable_instance – Deprecate or Fix?

Jon Baker

The MITRE Corporation

HS SEDI | MITRE
Homeland Security Systems Engineering and Development Institute

HS SEDI is a trademark of the U.S. Department of Homeland Security.
© 2011 The MITRE Corporation. All Rights Reserved.

Ambiguity in the definitions of @variable_instance

- **oval-results-schema.xsd DefinitionType and ExtendDefinitionType @variable_instance**
  - The optional variable_instance attribute is a unique id that differentiates each unique instance of a definition. Capabilities that use OVAL may reference the same definition multiple times and provide **different sets of variable values** each time the definition is referenced. This will result in multiple instances of a definition being included in the OVAL Results document (definitions that do not use variables can only have one unique instance). The inclusion of a unique instance identifier will allow the OVAL Results document to report the correct item associated with an object for each combination of supplied values.

- **oval-results-schema.xsd CriterionType @variable_instance TestType @variable_instance**
  - The optional variable_instance attribute differentiates between unique instances of a test. This can happen when a test includes a variable reference and **different values for that variable** are used by different definitions.

- **oval-system-characteristics-schema.xsd ObjectType @variable_instance**
  - The optional variable_instance identifier is a unique id that differentiates each unique instance of an object. Capabilities that use OVAL may reference the same definition multiple times and provide **different sets of variable values** each time the definition is referenced. This will result in multiple instances of an object being included in the OVAL System Characteristics file (definitions that do not use variables can only have one unique instance). **The inclusion of a unique instance identifier will allow the OVAL results file to report the correct item associated with an object for each combination of supplied values.**

© 2011 The MITRE Corporation. All Rights Reserved.

Confusion with Variable Values

- In OVAL a variable is a list of values
  - Each variable can have 0-n values

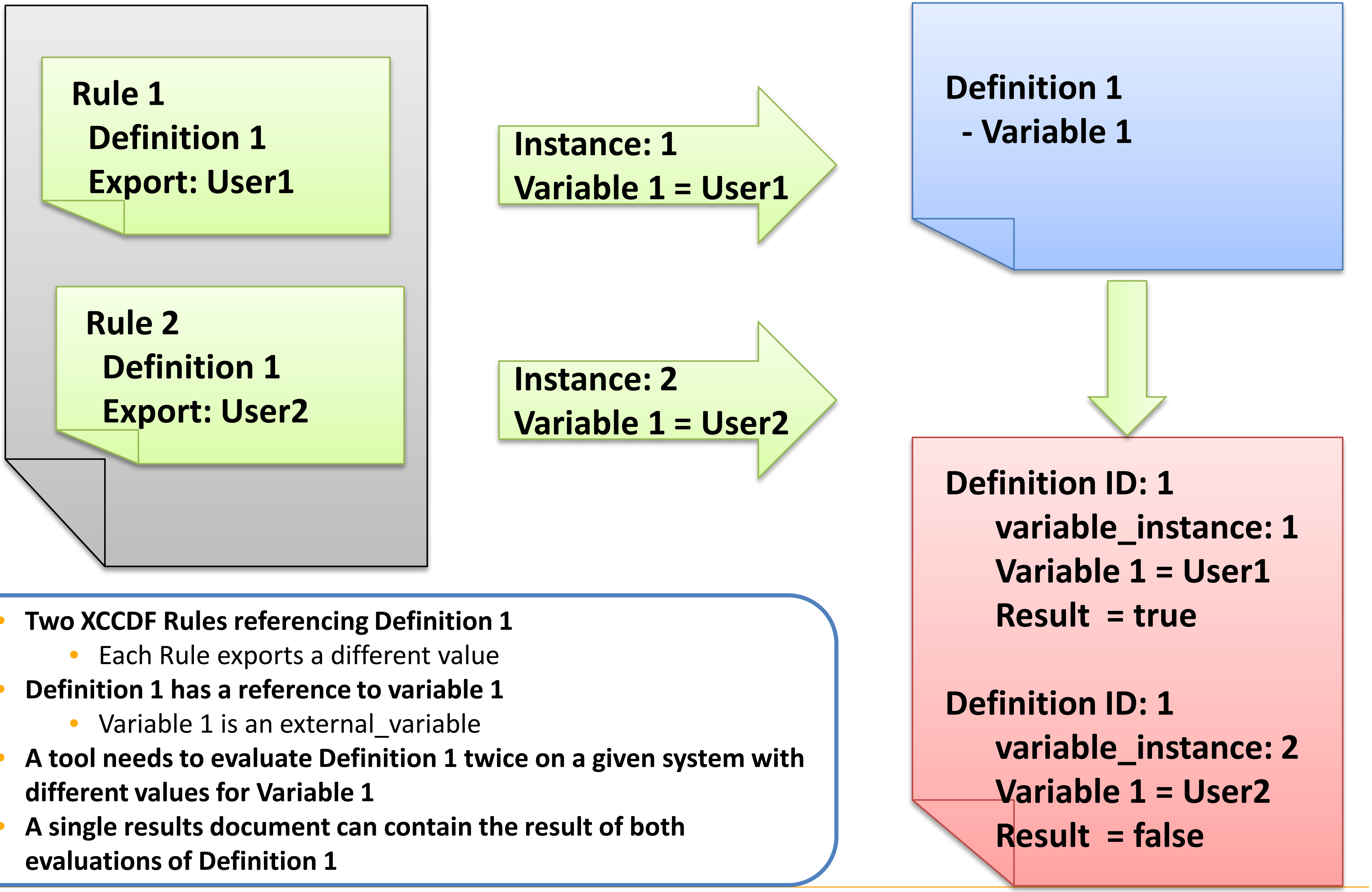
- The documentation inconsistently explains variable values
  - value(s)
  - array
  - set
  - multiple values

- @variable_instance documentation uses
  - “different sets of variable values”
  - “different values for that variable”

- Several oval-developer-list messages due to this confusion
  - Plenty of room for confusion here…

© 2011 The MITRE Corporation. All Rights Reserved.

Variable Instance Overview



Rule 1
Definition 1
Export: User1

Rule 2
Definition 1
Export: User2

Instance: 1
Variable 1 = User1

Instance: 2
Variable 1 = User2

Definition 1
- Variable 1

Definition ID: 1
variable_instance: 1
Variable 1 = User1
Result = true

Definition ID: 1
variable_instance: 2
Variable 1 = User2
Result = false

- **Two XCCDF Rules referencing Definition 1**
    - Each Rule exports a different value
- **Definition 1 has a reference to variable 1**
    - Variable 1 is an external_variable
- **A tool needs to evaluate Definition 1 twice on a given system with different values for Variable 1**
- **A single results document can contain the result of both evaluations of Definition 1**

© 2011 The MITRE Corporation. All Rights Reserved.

Sample Definition

```
<oval_definitions ...>
  ...
  <definitions>
    <definition id="oval:example:def:1" version="1" ...>
      ...
      <criteria>
        <criterion comment="VARIABLE is in the Administrators Group" test_ref="oval:example:tst:1"/>
      </criteria>
    </definition>
  </definitions>
  <tests>
    <user_test comment="VARIABLE is in the Administrators Group" id="oval:example:tst:1" version="1" ...>
      <object object_ref="oval:example:obj:1"/>
      <state state_ref="oval:example:ste:1"/>
    </user_test>
  </tests>
  <objects>
    <user_object comment="VARIABLE's group memberships" id="oval:example:obj:1" version="1" ...>
      <user var_check="at least one" var_ref="oval:example:var:1"/>
    </user_object>
  </objects>
  <states>
    <group_state comment="Member of Administrators group" id="oval:example:ste:1" version="1" ...>
      <group entity_check="at least one">Administrators</group>
    </group_state>
  </states>
  <variables>
    <external_variable comment="VARIABLE username to determine if the user is in the admin group"
           datatype="string" id="oval:example:var:1" version="1"/>
  </variables>
</oval_definitions>
```

© 2011 The MITRE Corporation. All Rights Reserved.

Two Instances Of Variable Values

Instance 1: Assign My-PC\User1 to oval:example:var:1

```
<oval_variables ...>
    ...
    <variables>
        <variable id="oval:example:var:1" datatype="string" comment=“A VARIABLE username">
            <value>My-PC\User1</value>
        </variable>
    </variables>
</oval_variables>
```

Instance 2: Assign My-PC\User2 to oval:example:var:1

```
<oval_variables ...>
    ...
    <variables>
        <variable id="oval:example:var:1" datatype="string" comment=“A VARIABLE username">
            <value>My-PC\User2</value>
        </variable>
    </variables>
</oval_variables>
```

© 2011 The MITRE Corporation. All Rights Reserved.

OVAL System Characteristics

```
<oval_system_characteristics ...>
  ...
  <collected_objects>
    <object id="oval:example:obj:1" variable_instance="1"
       comment="User VARIABLE's group memberships" flag="complete" version="1">
      <variable_value variable_id="oval:example:var:1">My-PC\User1</variable_value>
      <reference item_ref="1"/>
    </object>
    <object id="oval:example:obj:1" variable_instance="2"
       comment="User VARIABLE's group memberships" flag="complete" version="1">
      <variable_value variable_id="oval:example:var:1">My-PC\User2</variable_value>
      <reference item_ref="2"/>
    </object>
  </collected_objects>
  <system_data>
    <user_item id="1" ...>
      <user>My-PC\User1</user>
      <group>Administrators</group>
    </user_item>
    <user_item id="2" ...>
      <user>My-PC\User2</user>
      <group>Users</group>
    </user_item>
  </system_data>
</oval_system_characteristics>
```

© 2011 The MITRE Corporation. All Rights Reserved.

OVAL Results

```
<definitions>
  <definition definition_id="oval:example:def:1" variable_instance="1" result="true" version="1">
    <criteria operator="AND" result="true">
      <criterion test_ref="oval:example:tst:1" variable_instance="1" result="true" version="1"/>
    </criteria>
  </definition>
  <definition definition_id="oval:example:def:1" variable_instance="2" result="false" version="1">
    <criteria operator="AND" result="true">
      <criterion test_ref="oval:example:tst:1" variable_instance="2" result="false" version="1"/>
    </criteria>
  </definition>
</definitions>
<tests>
  <test test_id="oval:example:tst:1" version="1" variable_instance="1" result="true" ...>
    <tested_item item_id="1" result="true"/>
    <tested_variable variable_id="oval:example:var:1">My-PC\User1</tested_variable>
  </test>
  <test test_id="oval:example:tst:1" version="1" variable_instance="2" result="false" ...>
    <tested_item item_id=“2" result="false"/>
    <tested_variable variable_id="oval:example:var:1">My-PC\User2</tested_variable>
  </test>
</tests>
```

© 2011 The MITRE Corporation. All Rights Reserved.

Discussion Topics

- How widely used is the variable_instance attribute?
  - Are there any examples of content needing this capability?
  - Have any vendors implemented this capability?

- Is the variable_instance attribute a needed capability?
  - If not needed can we deprecate it?

- Clear need to clarify some of this documentation regardless of decision

© 2011 The MITRE Corporation. All Rights Reserved.