

Variable Manipulation Proposal

Contributors:
Ken.Lassesen@PatchLink.com
Kevin.Strietzel@PatchLink.com

Intellectual Property Statement

PatchLink grants the OVAL™ community an unrestricted use license for any content of this document when incorporated into OVAL™'s official schema and official standards.



1. Table of Contents

- 1. Table of Contents2
- 2. The Problem3
- 3. Demonstration Cases4
 - 3.1 c:\inetpub\Scripts,,204 4
- 4. Proposal.....6
- 5. Appendix: OVAL-DISCUSSION THREAD.....7
- 6. Revision History 10

2. The Problem

This document arose from a post on on the OVAL-DISCUSSION-LIST (see appendix for the tread).

It has been identified that there can be a legitimate need to do string manipulation beyond simple concatenation that is currently supported. There are several ways of approaching this such as:

- Xml Script¹
- XSL
- Embedded Scripting (XEXPR, XML Virgule, XOTcl etc)
- Regular Expressions.

One desirable OVAL objective is not to re-invent the wheel or require proprietary components. Since Pattern is a regular part of the definition schema, the use of regular expression automatically becomes a preferred situation. This document examines the feasibility of this preferred solution. The examples given will likely be extended over time to include other demonstration cases.

¹ <http://www.xmlscript.org/>

3. Demonstration Cases

The demonstration cases are done by using the RegExp engine in JavaScript for purposes of illustration only. There is an outstanding discussion on the ideal Regular Expression dialect engine, so JavaScript is used for illustration (***not*** prescriptive).

<http://www.regextester.com/> was used for testing.

3.1 c:\\inetpub\\Scripts,,204

Problem: The variable value “c:\\inetpub\\Scripts,,204” needs to be manipulated to “c:\\inetpub\\Scripts”.

Solution:

Figure 1 Obtaining the raw string

Dialect: JavaScript P_{re}g E_{re}g

Flags: i: g: m:

Type regex:

Test on Text:

Replace with:

Result:

Figure 2 Modifying the raw string

Dialect: JavaScript Preq Ereq

Flags: i: g: m:

Type regex:

`c:\inetpub\Scripts,,204`

Test on Text:

`c:\inetpub\Scripts,,204`

Replace with: Del

Result:

`c:\inetpub\Scripts\`

4. Proposal

It is purposed that for all variable elements three new attributes be added:

- @replacepattern [optional] string – the regular expression to be applied to the string
- @replace [optional] string – the replacement string
- @replaceref [optional] string – id of another variable.
 - This allows more complex string manipulation to be built up if needed.

The value of the contents (if it is a concatenation, then the post concatenation string).

The following is a contrived example for illustration only

```
<local_variable id="oval:org.mitre.oval:var:1" datatype="string" comment="Windows
system 32 directory" version="1">
  <concat replacepattern=":" replace=":">
    <object_component item_field="value" object_ref="oval:org.mitre.oval:obj:2"
      replacepattern=":" replaceref="oval:org.mitre.oval:obj:222323"
    />
    <literal_component >\system32</literal_component>
  </concat>
</local_variable>
```

5. Appendix: OVAL-DISCUSSION THREAD

[OVAL-DISCUSSION-LIST] Problem with variable oval:org.mitre.oval:var:205

4 messages

John Hoyland <jhoyland@centennial-software.com>

Wed, Aug 2, 2006 at 5:45 AM

Reply-To: OVAL Moderated Public Discussion List <OVAL-DISCUSSION-LIST@lists.mitre.org>

To: OVAL-DISCUSSION-LIST@lists.mitre.org

Hi folks,

We think there is a problem with the variable oval:org.mitre.oval:var:205:

```
<local_variable id="oval:org.mitre.oval:var:205" datatype="string"
comment="Windows system 32 directory" version="1">
```

```
  <concat>
    <object_component item_field="value"
object_ref="oval:org.mitre.oval:obj:219"/>
    <literal_component>InetPub\scripts\proxy</literal_component>
  </concat>
</local_variable>
```

This uses the object oval:org.mitre.oval:obj:219:

```
<registry_object id="oval:org.mitre.oval:obj:219" 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>SystemRoot</name>
</registry_object>
```

Which gives us the Windows directory e.g. "C:\WINDOWS\".

From what we've seen (which may not be a representative sample of installations), the Inetpub directory is usually a top-level directory e.g. "C:\Inetpub", and not a sub-directory of the Windows directory.

A possibility for re-writing this would be to create a new registry object:

```
<registry_object id="oval:org.mitre.oval:obj:XXXX" version="1"
xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
  <hive>HKEY_LOCAL_MACHINE</hive>
  <key>SYSTEM\CurrentControlSet\Control\ContentIndex\Catalogs\Web</key>
  <name>Location</name>
</registry_object>
```

On a couple of machines here, this contains the Inetpub directory e.g. "c:\inetpub". If this is a reliable way to get the Inetpub directory then the variable could be re-written to

use this object:

```
<local_variable id="oval:org.mitre.oval:var:205" version="2" datatype="string"
comment="InetPub\scripts\proxy directory">
```

```
  <concat>
    <end character="\ ">
    <object_component item_field="value"
object_ref="oval:org.mitre.oval:obj:XXXX"/>
  </end>
  <literal_component>scripts\proxy</literal_component>
</concat>
</local_variable>
```

However, I don't really have enough evidence to know whether this solution is general enough. Does anyone else have any ideas on this?

regards,

John Hoyland

Important Note: This email is confidential and may be privileged. It is intended solely for its addressee. Access and/or use by others is unauthorised and may be unlawful. If you receive this mail in error, please report the incident. All email sent to or from this address is subject to archival and review by someone other than the recipient.

To unsubscribe, send an email message to LISTSERV@LISTS.MITRE.ORG with SIGNOFF OVAL-DISCUSSION-LIST in the BODY of the message. If you have difficulties, write to OVAL-DISCUSSION-LIST-request@LISTS.MITRE.ORG.

Ken Lassesen <ken.lassesen@gmail.com>

Wed, Aug 2, 2006 at 7:56 AM

To: OVAL Moderated Public Discussion List <OVAL-DISCUSSION-LIST@lists.mitre.org>

To me, the location should use

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots]
"/Scripts"
```

The "Scripts" folder is where it must be located -- wherever that is located.... it does not need to be under C:\inetPub\

As a FYI On my machine I have the following three references...

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\W3SVC\Parameters\Virtual Roots]
"/Scripts"="c:\inetpub\Scripts,,204"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services\W3SVC\Parameters\Virtual Roots]
"/Scripts"="c:\inetpub\Scripts,,204"
```

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC\Parameters\Virtual Roots]
"/Scripts"="c:\inetpub\Scripts,,204"
```

[Quoted text hidden]

--

Ken Lassenen
MSNMessenger: Ken@Lassenen.com
Office: 360-297-4717 Cell:360-509-2402
<http://www.linkedin.com/pub/1/4a/841>

John Hoyland <jhoyland@centennial-software.com>

Fri, Aug 4, 2006 at 3:21 AM

Reply-To: OVAL Moderated Public Discussion List <OVAL-DISCUSSION-LIST@lists.mitre.org>
To: OVAL-DISCUSSION-LIST@lists.mitre.org

That would be an excellent solution except that the available functions for variable processing don't seem sufficient to remove the trailing ",,204". Providing more and/or enhanced functions in this area seems like another good idea for the next version.

regards,

John Hoyland

From: Ken Lassenen [mailto:ken.lassenen@GMAIL.COM]

Sent: 02 August 2006 15:57

To: OVAL-DISCUSSION-LIST@LISTS.MITRE.ORG

Subject: Re: [OVAL-DISCUSSION-LIST] Problem with variable oval:org.mitre.oval:var:205

[Quoted text hidden]

<http://www.linkedin.com/pub/1/4a/841> To unsubscribe, send an email message to LISTSERV@LISTS.MITRE.ORG with SIGNOFF OVAL-DISCUSSION-LIST in the BODY of the message. If you have difficulties, write to OVAL-DISCUSSION-LIST-request@LISTS.MITRE.ORG. Important Note: This email is confidential and may be privileged. It is intended solely for its addressee. Access and/or use by others is unauthorised and may be unlawful. If you receive this mail in error, please report the incident. All email sent to or from this address is subject to archival and review by someone other than the recipient.

[Quoted text hidden]

Ken Lassenen <ken.lassenen@gmail.com>

Fri, Aug 4, 2006 at 9:41 AM

To: OVAL Moderated Public Discussion List <OVAL-DISCUSSION-LIST@lists.mitre.org>

If you don't object (feel free to pick it up if you wish), I will investigate this a bit and write up a proposal to kick off discussion of the issue you raised.

[Quoted text hidden]

6. Revision History

Version	Date	Author(s)	Description
1.0	2005-08-04	Ken Lassenen	• Initial Version

Intellectual Property Caveat

The contents of this document may include concepts, algorithms or methodologies that may be the subject of one or more patent applications.