Proposed OVAL Updates For Microsoft Internet Information Server (IIS) Settings
Using AppCmd.exe - appcmd Test

March 15, 2017
Version: 1.0

1. Background

OVAL 5.11.2 lacks a robust, straight-forward, and efficient mechanism to query Microsoft Internet Information Server (versions 7.0 – 10) configuration settings. The existing OVAL cmdlet test is inadequate as it fails to provide adequate data resolution. For instance, if an Internet Information Server (IIS) installation hosts multiple websites, the cmdlet test results do not enable the user to determine from which website a reported setting was collected.

The Microsoft AppCmd.exe application is the primary method for querying and managing IIS servers. We propose two new OVAL tests, the appcmd and appcmdlistconfig tests to query IIS data using AppCmd.exe.

This document defines the proposed appcmdlistconfig test. See an accompanying proposal covering the appcmd test.

1.1. AppCmd.exe Information

Please review the following link for information on AppCmd.exe. The two new OVAL tests both utilize AppCmd.exe List Command.

https://www.iis.net/learn/get-started/getting-started-with-iis/getting-started-with-appcmdexe

1.2. Two OVAL Tests – appcmd and appcmdlistconfig

The appcmd and appcmdlistconfig OVAL tests utilize the *AppCmd.exe LIST* system command. When using *AppCmd.exe*, certain settings are available using the Site, *Apppool* or *VDir* objects (in scope for the appcmd test) and other settings are available using the *Config* object (in scope for the appcmdlistconfig test). The following table shows what settings are "available" for each test (an X indicates settings can be gathered via referenced test).

IIS Settings Available Per Test		
Settings	**appcmd test**	**appcmdlistconfig test**
Webserver		X
Website (Site)	X	X
Virtual Directory (VDir)	X	X
Application Pool (Apppool)	X	

2. Summary

This section defines the OVAL appcmd test, object, and state. The appcmd_test references the appcmd_object and the appcmd_state. The following tables define the appcmd_object, appcmd_state, and appcmd_item.

appcmd_object	
Element	**Notes**
object	Must be set to [Apppool, Site, VDir]
identifier	Defines the object instance
parameter	Defines location of setting

appcmd_state	
Element	**Notes**
object	Must be set to [Apppool, Site, VDir]
identifier	Defines the object instance
parameter	Defines location of setting
result_descriptor	Location of the found result
result_value	Collected value

appcmd_item	
Element	**Notes**
object	Must be set to [Apppool, Site, VDir]
identifier	Defines the object instance
parameter	Defines location of setting
result_descriptor	Location of the found result
result_value	Collected value

2.1. *AppCmd.exe* command generated from appcmd test OVAL Object

The following pseudo code shows how an appcmd_object is converted to an AppCmd.exe command. Names in all-capitals are variables defined in content.

- appcmd_object in OVAL content (pseudo code)

```
<appcmd_object>
        <object>OBJECT</object>
        <identifier operation="pattern match">IDENTIFIER</identifier>
        <parameter>PARAMETER</parameter>
</appcmd_object>
```

- AppCmd.exe command generated from valid content

  AppCmd.exe list OBJECT IDENTIFIER /text:PARAMETER
  - The identifier in the command is generated based on content identifier type and identifier setting. To review all, a pattern match with IDENTIFIER equal to ".*"

3. New Capabilities that Cannot Currently be Accomplished with OVAL

The appcmd test will allow review of IIS settings that currently cannot be gathered via existing OVAL tests.

4. Relevance of the New Capability

This update would be relevant to Windows only and only to content using OVAL 5.12 and later.

5. Impact upon OVAL Content Developers

Content Developers will have OVAL tests that can be used to gather IIS configuration settings.

6. Impact upon OVAL Content Consumers

Once content is available, content consumers can obtain OVAL tests that can be used to gather IIS configuration settings. Content processors will need to be extended to support the new test type.

7. Impact upon Existing OVAL Content

None.

8. Impact upon Existing OVAL Implementations

Same as #6.

9. Relevance to Existing OVAL Use Cases

None

10. Affected OVAL Schema Documents

- windows-definitions-schema.xsd
- windows-system-characteristics-schema.xsd

11. Backward Compatibility with Previous Versions

None.

12. Demonstration of the New Capabilities

The addition of the appcmd test has been demonstrated with a pre-release version of the SCAP Compliance Checker 4.2. Sample schema update, content, and sample results are available for review.

This section's content is intended for content authors.

12.1. Notes Regarding Included Sample appcmd OVAL Content

This document presents two example content files:

- appcmd_test-oval_Prototype_ForForum.xml
- appcmd_test-oval_Prototype_ForForum_DISAExamples.xml

These documents can be found in content directory included with this prototype.

12.1.1. appcmd_test-oval_Prototype_ForForum Definitions

The file “appcmd_test-oval_Prototype_ForForum.xml” contains the following OVAL test examples.

- tst:1 Application Pool Setting - all application pools reviewed
- tst:2 Application Pool Setting - subset of application pools reviewed via regular expression (set in identifier)
- tst:3 Application Pool Setting - subset of application pools reviewed via equal to (set in identifier) 'DefaultApppool' which exists by default.
- tst:4 Application Pool Setting - subset of application pools reviewed via not equal to (set in identifier) 'DefaultApppool' which exists by default.
- tst:5 Website Setting - all websites reviewed
- tst:6 Website Setting - subset of websites reviewed via regular expression (set in identifier)
- tst:7 VDir Setting - all virtual directories reviewed
- tst:8 Not Collected - Incorrect Parameter Example - AppCmd.exe reports error due to incorrect parameter setting.
- tst:9 Not Collected - Application Pool 'Equals' (set in identifier) 'Non-Matching-String' - no application pools named 'Non-Matching-String'
  - tst:8 and tst:9 are both repeats of tst:8 with key differences. Both tests result in “Not Collected”.
  - tst:8 has the parameter is set to an invalid (nonexistent) string.
  - tst:9 has the identifier operation of equals and identifier set to a website that doesn’t exist on target system.

12.1.2. appcmd_test-oval_Prototype_ForForum_DISAExamples Definitions

“appcmd_test-oval_Prototype_ForForum_DISAExamples.xml” – 3 Definitions

- tst:1 Application Pool Setting Example - STIG ID: WA000-WI6028 IIS7 - The Idle Timeout monitor shall be enabled and set to 20 minutes.
- tst:2 Website Setting Example - STIG ID: WG110 IIS7 - Web sites must limit the number of simultaneous requests.
- tst:3 Application Pool Setting Example - STIG ID: WA000-WI6034 IIS7 - An application pool’s rapid fail protection must be enabled.

Note: All tests referenced in IIS 7.0 STIG - Ver 1, Rel 12. Settings defined in this STIG are application for all versions of IIS after version 7.0.

12.2. Notes Regarding Example of SCC Results From OVAL Content

SCAP Compliance Checker (SCC) results, with content noted in previous section, is included. The results directory included with this prototype the following subfolders:

12.2.1. appcmd_test-oval_Prototype_ForForum Results

- tst:1 – tst:4 show results from a test server which has two application pools. By examining results one can see how a content author can form content that will review all application pools or a subset of application pools.
- tst:5 and tst:6 are examples of reviewing websites. The same examination of results will again show how all or a subset of websites can be examined.
- tst:7 shows that two VDirs were reviewed and data was successfully gathered.
- tst:8 and tst:9 are examples of content resulting in a not collected item.

12.2.2. appCmd_test-oval_Prototype_ForForum_DISAExamples Results

- The results for the three checks that are related to DISA content are included.
- Examples included are two requirements which required all application pools to be reviewed and one example of a requirement that reviews all websites. Please review results included.

13. OVAL Schema Update

Two .xsd files are included in this proposal, “appcmd_updates_windows-definitions-schema.xsd” and “appcmd_updates_windows-system-characteristics-schema.xsd” are the schema for the new test, object and state.