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

March 14, 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 appcmdlistconfig test, object, and state. The appcmdlistconfig_test references the appcmdlistconfig_object and the appcmdlistconfig_state. The following tables define the appcmdlistconfig_object, appcmdlistconfig_state, and appcmdlistconfig_item.

appcmdlistconfig_object	
Element	**Notes**
identifier_type	Must be set to [Webserver, Site, VDir]
identifier	Defines the object instance
section	Defines section of setting
parameter	Defines location of setting

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

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

2.1. AppCmd.exe command generated from appcmdlistconfig test content

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

- appcmdlistconfig test – appcmdlistconfig_object in OVAL content (pseudo code)

```
<appcmdlistconfig_object>
        < identifier_type>IDENTIFIER_TYPE</ identifier_type>
        <identifier operation="pattern match">IDENTIFIER</identifier>
        <section>SECTION</section>
        <parameter>PARAMETER</parameter>
</appcmdlistconfig_object>
```

- AppCmd.exe command generated from valid content

  AppCmd.exe list config IDENTIFIER_TYPE /section:SECTION /text:PARAMETER
  - The identifier in the command is generated based on content identifier type and identifier setting (see regular expression talk in this section).

3. New Capabilities that Cannot Currently be Accomplished with OVAL

The appcmdlistconfig 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 #5.

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 appcmdlistconfig OVAL capability 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.

Please note that this section's content is more directed at content authors.

12.1. Notes Regarding Included Sample appcmdlistconfig OVAL Content

This document will present two example content files:

- appcmdlistconfig_test-oval_Prototype_ForForum.xml
- appcmdlistconfig_test-oval_Prototype_ForForum_DISAExamples.xml

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

12.1.1. appcmdlistconfig_test-oval_Prototype_ForForum Definitions

"appcmdlistconfig_test-oval_Prototype_ForForum.xml" – 9 Definitions

- tst:1: Website Setting - All Websites Reviewed
- tst:2: Website Setting - Subset Of Websites Reviewed via regular expression (set in identifier)
- tst:3: Website Setting - Subset Of Websites Reviewed via equal to (set in identifier)
- tst:4: Website Setting - Subset Of Website Reviewed via not equal to (set in identifier)
- tst:5: VDir Setting - All Virtual Directories Reviewed
- tst:6: VDir Setting Example - Subset Of VDir's Reviewed via regular expression (set in identifier)
- tst:7: Webserver Setting Example
- tst:8: Not Collected – Incorrect Parameter Example - AppCmd.exe reports error due to incorrect parameter setting.
- tst:9: Not Collected – Incorrect Section Example - AppCmd.exe reports error due to incorrect parameter setting.
  - tst:8 and tst:9 are both repeats of tst:5 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 section is set to an invalid (nonexistent) string

12.1.2. appcmdlistconfig_test-oval_Prototype_ForForum_DISAExamples Definitions

"appcmdlistconfig_test-oval_Prototype_ForForum_DISAExamples.xml" – 4 Definitions

- tst:101: Website Setting Example - STIG ID: WA000-WI6140 IIS7 - Debug must be turned off on a production website
- tst:102: Website Setting Example - STIG ID: WA000-WI6240 - The web-site must not allow non-ASCII characters in URLs.
- tst:103: Webserver Setting Example - STIG ID: WA000-WI6100 - Unspecified file extensions must not be allowed to execute on the production web server. (1 of 2)
- tst:104: Webserver Setting Example - STIG ID: WA000-WI6100 - Unspecified file extensions must not be allowed to execute on the production web server. (2 of 2)

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 are included. The results directory included with this prototype the following subfolders:

12.2.1. appcmdlistconfig_test-oval_Prototype_ForForum Results

- tst:1-4 are results from a test server which has two websites. By examining results one can see how a content author can form content that will review all websites or a subset of websites.
- tst:5 and tst:6 are examples of reviewing virtual directories. The same examination of results will again show how all or a subset of virtual directories can be examined.
- tst:7 is an example of an examination of a webserver setting. Since the identifier_type is set to Webserver the identifier is not needed in content and not part of the collected item.
- tst:8 and tst:9 are examples of content resulting in a not collected item.

12.2.2. appcmdlistconfig_test-oval_Prototype_ForForum_DISAExamples Results

- The results for the four checks that are related to DISA content are included. As noted earlier requirements from the IIS 7.0 STIG (Ver 1, Rel 12) were used as examples to show the appcmdlistconfig test can be used to review IIS servers.
- Examples included are two requirements which required all websites to be reviewed and two examples of requirements that are applicable to webserver configuration settings. Please review results included.

13. OVAL Schema Update

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