Microsoft

SCAP Vendor Assertion Document

SCAP Extensions for System Center Configuration Manager

Version 3.0

Technical White Paper
7/15/2015

Table of Contents

Assertion 3

SCAP Implementation Statement 3

SCAP 1.2 Conformance 6

SCAP 1.1 Compatibility 6

SCAP 1.0 Compatibility 6

Copyright Information

Assertion

Microsoft Corporation Inc. asserts that the SCAP Extensions version 3.0 for Microsoft System Center Configuration Manager meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.0, 1.1, and 1.2, as described in NIST IR 7511 Revision 3 for the following SCAP capabilities and supported platform families:

Capabilities

Authenticated Configuration Scanner

Common Vulnerabilities and Exposures (CVE) Option

Platform Families

Microsoft Windows 7, 32- and 64-bit

SCAP Implementation Statement

Compliance settings in Microsoft System Center Configuration Manager provides a unified interface and user experience that lets you manage the configuration and compliance of servers, laptops, desktop computers, and mobile devices in your organization. Compliance settings contains tools to help you assess the compliance of users and client devices for many configurations, such as whether the correct Windows operating system versions are installed and configured appropriately, whether all required applications are installed and configured correctly, whether optional applications are configured appropriately, and whether prohibited applications are installed. Additionally, you can check for compliance with software updates, security settings, and mobile devices.

Compliance is evaluated by defining a configuration baseline that contains the configuration items that you want to evaluate and settings and rules that describe the level of compliance you must have. You can import this configuration data or, an administrative user can create new configuration items and configuration baselines.

After a configuration baseline is defined, you can deploy it to users and devices through collections and evaluate its settings for compliance on a schedule. Client devices can have multiple configuration baselines deployed to them. This provides the administrator with a high level of control.

Client devices evaluate their compliance against each deployed configuration baseline and immediately report the results to the site by using state messages and status messages. You can monitor the results of the configuration baseline evaluation compliance in the Configuration Manager console to view the most common causes of noncompliance, errors, and the number of users and devices that are affected.

You can use compliance settings to support the following business requirements:

- Compare the configuration of desktop computers, laptops, servers, and mobile devices in your enterprise against best practices configurations from Microsoft and other vendors.
- Report compliance with regulatory policies and in-house security policies.
- Verify the configuration of provisioned devices against one or more custom-defined configuration baselines before the computers go into production.
- Remediate noncompliance by deploying applications, packages and programs, or scripts to a collection that is automatically populated with computers that report that they are out of compliance.

For more information about ***Compliance Settings in Configuration Manager*** please see https://technet.microsoft.com/en-us/library/gg681958.aspx

USGCB

The SCAP Extensions version 3.0 for System Center Configuration Manager use the Compliance Settings feature in System Center Configuration Manager to scan the computers in your environment and then document their level of compliance with the United States Government Configuration Baseline (USGCB) mandate.

The SCAPToDCM tool lets you convert SCAP data stream files to Configuration Manager Compliance Settings .cab files. SCAPToDCM will derive the settings and rules from the CVE, CCE, CPE, XCCDF and OVAL content and create the appropriate configuration baselines inside the cab file.

You can import the cab files using the Configuration Manager console and then deploy the configuration baselines to your Configuration Manager client devices where the tests will be executed. These will be returned to the Configuration Manager site server where the results are evaluated and you can monitor compliance in the Configuration Manager console by using the monitoring workspace or by running compliance settings reports.

You can use the DCMToSCAP tool to export reports in SCAP compliant ARF format.

XCCDF

XCCDF (eXtensible Common Configuration Data Format) is a specification language for writing security checklists, benchmarks and related types of documents, as defined by NIST.

The SCAP Extensions version 3.0 for System Center Configuration Manager provides support for reading, validating and converting/importing files that contain XCCDF data. When working with a SCAP 1.2 data stream file or a SCAP 1.0/1.1 XCCDF file you can identify the specific XCCDF benchmark or profile for the SCAPToDCM tool to convert to a configuration baseline. The DCMTOSCAP tool generates XCCDF results.

OVAL

Open Vulnerability and Assessment Language (OVAL) is an international information security standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

The SCAP Extensions version 3.0 for System Center Configuration Manager supports OVAL compliance checking by allowing you to import OVAL checks (standalone and/or SCAP data streams) from the OVAL repository,

- Allows selection of a standalone OVAL file or an OVAL file paired with an OVAL external variable file.
- Uses Windows PowerShell scripts instead of VBScripts in the Configuration Items for all OVAL test types.
- Generates OVAL results embedded in the ARF results files.

CCE

Common Configuration Enumeration (CCE) is a dictionary of names for software security configuration issues (e.g., access control settings, password policy settings). As such, CCEs describe system configuration issues to facilitate correlation of configuration data across multiple information sources and tools.

The SCAP Extensions version 3.0 for System Center Configuration Manager supports CCE by displaying the CCE ID in the ARF report. If there is a CCE ID a human readable report will be generated also. This includes the required output format defined as "CCE ID, pass/fail"

CPE

CPE (Common Platform Enumeration) is a structured naming scheme for information technology systems, software and packages.

The SCAP Extensions version 3.0 for System Center Configuration Manager supports CPE by converting CPE content to a platform applicability in Configuration Manager. The CPE results are contained in the ARF report.

CVE

CVE (Common Vulnerabilities and Exposures) is a dictionary of publicly known information security vulnerabilities and other information security exposures.

The SCAP Extensions version 3.0 for System Center Configuration Manager supports CVE by displaying the CVE ID in the ARF report. If there is a CVE ID a human readable report will be generated also. This includes the required output format defined as "CVE ID, pass/fail"

Asset Reporting Format (ARF)

The Asset Reporting Format (ARF), under SCAP, expresses the transport format of information about assets and the relationships between assets and reports.

The SCAP Extensions version 3.0 for System Center Configuration Manager supports the ARF specification, by generating ARF-formatted output using the DCMToSCAP tool.

SCAP 1.2 Conformance

SCAP Extensions version 3.0 for System Center Configuration Manager conforms to the specifications of the Security Content Automation Protocol, version 1.2 (SCAP 1.2), as outlined in NIST Special Publication (SP) 800-126 rev 2.

- Fully supports converting SCAP Content to Compliance Settings baselines for System Center 2012 Configuration Manager SP1 and System Center 2012 R2 Configuration Manager.
- Supports Extensible Configuration Checklist Description Format (XCCDF) version 1.2.
- Supports Open Vulnerability and Assessment Language (OVAL) versions up to 5.10.
- Supports generating Asset Reporting Format (ARF) 1.1 reports.
- Supports Common Platform Enumeration (CPE) 2.3
- Supports Common Vulnerabilities and Exposures (CVE)
- Supports Common Configuration Enumeration (CCE) version 5
- Supports USGCB Internet Explorer 8, USGCB Windows 7 and USGCB Windows 7 Firewall

SCAP 1.1 Compatibility

- Supports Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4.
- Supports Open Vulnerability and Assessment Language (OVAL) versions 5.3 and 5.4.
- Supports Common Platform Enumeration (CPE) 2.2
- Supports Common Vulnerabilities and Exposures (CVE)
- Supports Common Configuration Enumeration (CCE) version 5
- Supports USGCB Internet Explorer 8, USGCB Windows 7 and USGCB Windows 7 Firewall

SCAP 1.0 Compatibility

- Supports Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4.
- Supports Open Vulnerability and Assessment Language (OVAL) versions 5.3 and 5.4.
- Supports Common Platform Enumeration (CPE) 2.2
- Supports Common Vulnerabilities and Exposures (CVE)
- Supports Common Configuration Enumeration (CCE) version 5
- Supports USGCB Internet Explorer 8, USGCB Windows 7 and USGCB Windows 7 Firewall

Additionally the SCAP Extensions 3.0 for Microsoft System Center Configuration Manager provides the following functionality which is not part of the certification process.

- Supports generating the Cyberscope Lightweight Asset Summary Results (LASR) report.

You will find more information about the features and functionality in *The SCAP Extensions version 3.0 for System Center Configuration Manager User Guide* http://go.microsoft.com/fwlink/?LinkID=526814&clcid=0x409.