Security Content Automation Protocol (SCAP)

SCAP Vendor Assertions Document v4.0

February 4, 2016

By

IBM
1480 64th St
Suite 200
Emeryville, CA, United States of America
94608

http://support.bigfix.com/product/documents/SCAP_QuickStart_Guide.pdf

For

IBM BigFix Compliance - SCAP

Version 9.2, CPE 2.3

Assertion:

IBM asserts that IBM BigFix Compliance - SCAP version 1016 meets or exceeds the Derived Test Requirements (DTR) for SCAP 1.2 as described in NIST IR 7511, Revision 3 for the following SCAP capabilities and supported platform family:

Capabilities:

- [X] Authenticated Configuration Scanner
- [X] CVE
- [ ] OCIL

Platform Family:

- [ ] Windows XP Professional SP3 (32 bit edition)
- [ ] Windows Vista SP2 (32 bit edition)
- [ ] Windows 7 SP1 (32 bit edition)
- [ ] Windows 7 SP1 (64 bit edition)
- [X] Red Hat Enterprise Linux 5 Desktop (32 bit edition)
- [X] Red Hat Enterprise Linux 5 Desktop (64 bit edition)

SCAP Component Technologies:

The following table provides a brief summary of the individual SCAP Component Standards supported by IBM BigFix Compliance - SCAP:

Supported	Component	Version	Description
✓	AI	1.1	Asset Identification (AI) is a specification for identifying assets
✓	ARF	1.1	The Asset Reporting Format (ARF) is a specification describing a data model for asset reporting
✓	CCE	5	The Common Configuration Enumeration ™ (CCE) is a nomenclature and dictionary of software security configurations
✓	CCSS	1.0	The Common Configuration Scoring System (CCSS) is a specification for measuring the relative severity of system security configuration issues
✓	CPE	2.3	The Common Platform Enumeration (CPE) is a specification measuring the relative severity of system security configuration issues
✓	CVE	n/a	The Common Vulnerability Enumeration® (CVE) is a specification describing a nomenclature and dictionary of security-related software flaws
-	CVSS	2.0	The Common Vulnerability Scoring System is a language for representing system configuration information, assessing machine state, and reporting assessment results
-	OCIL	2.0	The Open Checklist Interactive Language (OCIL) is a language for representing checks that collect information from people or from existing data stores made by other data collection efforts
✓	OVAL	5.10.1	The Open Vulnerability and Assessment Language is a language for representing system configuration information, assessing machine state, and reporting assessment results
✓	SCAP	1.2	SCAP is a specification for expressing and manipulating security data in standardized ways. SCAP uses several individual specifications in concert to automate continuous monitoring, vulnerability management, and security policy compliance evaluation reporting
-	TMSAD	1.0	The trust Model for Security Automation Data (TMSAD) describes a common trust model that can be applied to specifications within the security automation domain
✓	XCCDF	1.2	Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents

SCAP Implementation Statement(s):

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation.

The IBM BigFix Compliance product supports the use of SCAP to generate mis-configuration, vulnerability, and patch based assessment rules so organizations can discover and report on software vulnerabilities, assess the impact of those vulnerabilities, enumerate and remediate the mis-configurations identified, and report on the current state of a system based on the SCAP defined policy definitions. IBM BigFix Compliance consumes a SCAP-expressed data stream, produces a set of policies known as Fixlet messages, and delivers real-time assessment and remediation on a global scale.

IBM BigFix Compliance managed systems continuously discover, assess, secure and remediate themselves according to an organization's SCAP-based policies and practices as well as the operating context in which it finds itself – mobile, connected, disconnected, etc. Without requiring significant investments in dedicated hardware, management resources, or professional services, IBM BigFix Compliance automates enterprise-scale desktop and server management, malware defenses, and IT policy enforcement without compromising network performance, end-user productivity, or security. IBM BigFix Compliance delivers superior, customer-documented, return-on-investment by reducing labor and infrastructure costs and automating critical management functions.

The Extensible Configuration Checklist Description Format (XCCDF) is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems and is the core element to the SCAP-expressed data stream. The specification also defines a data model and format for storing benchmark compliance testing results. One of the many features of the Security and Compliance product includes the ability to consume an SCAP-Expressed data stream, which includes the XCCDF component, and translate the underlying configuration checks that are defined into IBM BigFix-compatible Fixlet messages. These Fixlet messages enable administrators to assess their computing assets against the SCAP defined configuration rules in real-time across one, thousands, or hundreds of thousands of endpoints regardless of location.

Once the SCAP converted configuration rules are imported into the IBM BigFix Console, any system under IBM BigFix management control, both on the managed network and off the managed network, can begin to immediately assess themselves against the defined configuration rules. The results of those configuration checks are relayed to the IBM BigFix Console where administrators can view the results and generate detailed reports on an individual system or large groups of systems in the aggregate.

IBM BigFix Compliance also provides the ability to export the results of the configuration checks into Asset Report Format (ARF) such that the organization can easily store those reports or send the report to another party.

BigFix provides the ability to generate CVE results. Users can view the results in an.xml file that includes CVE information, including the status of the check and the CVE identifiers. The CVE ID has links to the corresponding vulnerability in the National Vulnerability Database (NVD) site.

BigFix also includes the ability to support CCSS scores. This is done by using a flat unweighted scoring when that score is used in the weight attribute within XCCDF rules.

SCAP Backwards Compatibility:

IBM BigFix Compliance consumes a SCAP-expressed data stream, produces a set of policies known as

Fixlet messages, and delivers real-time assessment and remediation on a global scale. The BigFix Compliance product for SCAP 1.2 is backwards compatible with SCAP 1.0 and SCAP 1.1. For SCAP 1.0, the tool is to be used through the "Import SCAP Content" wizard to output XCCDF format. For SCAP 1.1, the content can be consumed by the SCAP 1.2 tool to output SCAP 1.2 Asset Reporting Format (ARF). To use the tool with SCAP 1.2 content, a "--benchmark" flag has been added.

The IBM BigFix Compliance product can be used with SCAP 1.0 and 1.1 data streams.
The flags to import SCAP 1.0 and 1.1 content through the SCAP tool are the same as SCAP 1.2 content, except that the "–benchmarks" flag does not need to be specified and the reporting output will be in SCAP 1.2 ARF.

In order to get SCAP 1.0 output in XCCDF form for an SCAP 1.0 data stream, the SCAP 1.0 tool is to be accessed and used through the "Import SCAP Content" wizard.

Disclaimer: