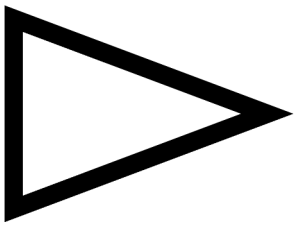
TECHNICAL WHITE PAPER



BMC Server Automation -
SCAP Implementation Statement

bmcsoftware
BUSINESS RUNS ON I.T.™

SCAP Implementation Statement

The SCAP features in BMC Server Automation comply with the Technical Specification for the Security Content Automation Protocol (SCAP): Version 1.2. Using features in the BMC Server Automation Console, you import SCAP content from third-party sources, such as the NIST NVD National Checklist Program repository. Results are generated as XML files compliant with both the SCAP (for ARF) and XCCDF specifications.

BMC Software, Inc. asserts that BMC Server Automation version 8.6.00 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
- Open Checklist Interactive Language (OCIL) Option

Platform Families

- Microsoft Windows 7, 64-bit
- Red Hat Enterprise Linux 5 Desktop, 64-bit

BMC Server Automation additionally provides SCAP capabilities for systems such as AIX, HP UX, Solaris, and other Windows/Linux flavors, but these are not certified.

SCAP 1.2 Conformance

BMC Server Automation 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. As part of the SCAP 1.2 protocol, BMC Server Automation assessment capabilities have been expanded to include the consumption of source data stream collection XML files and the generation of well-formed SCAP result data streams.

To exercise this capability, users may download the SCAP 1.2 content from the NIST NVD National Checklist Program repository, or any other source of SCAP 1.2 compliant content, and perform SCAP compliance assessments in BMC Server Automation.

The BMC Server Automation implementation includes the following components:

- Extensible Configuration Checklist Description Format (XCCDF) 1.2, a language for authoring security checklists/benchmarks and for reporting results of evaluating them.
- Open Vulnerability and Assessment Language (OVAL) 5.10, a language for representing system configuration information, assessing machine state, and reporting assessment results.
- Open Checklist Interactive Language (OCIL) 2.0 defines a framework for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions. OCIL is especially suited for expressing and evaluating non-automated (that is, manual) security checks.
- Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about assets and the relationships between assets and reports.
- Asset Identification 1.1, a format for uniquely identifying assets based on known identifiers and/or known information about the assets.
- Common Platform Enumeration (CPE) 2.3, a nomenclature and dictionary of hardware, operating systems, and applications.

- Common Configuration Enumeration (CCE) 5, a nomenclature and dictionary of software security configurations.
- Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaws.
- Common Vulnerability Scoring System (CVSS) 2.0, a system for measuring the relative severity of software flaw vulnerabilities.
- Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of system security configuration issues. BMC Server Automation supports CCSS scores when that score is used in the @weight attribute within XCCDF rules.
- Trust Model for Security Automation Data (TMSAD) 1.0, a specification for using digital signatures in a common trust model applied to other security automation specifications. BMC Server Automation can import SCAP content with Trust Model for Security Automation Data (TMSAD) signatures but will not verify them. The generated XML report will not include TMSAD signatures.

SCAP 1.0 Compatibility

BMC Server Automation natively supports the older SCAP 1.0 specification, including:

- Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4
- Open Vulnerability and Assessment Language (OVAL), version 5.3 and 5.4
- Common Configuration Enumeration (CCE) version 5
- Common Platform Enumeration (CPE) version 2.2
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) version 2.0

SCAP 1.1 Compatibility

BMC Server Automation natively supports the older SCAP 1.1 specification, including:

- Extensible Configuration Checklist Description Format (XCCDF) version 1.1.4
- Open Vulnerability and Assessment Language (OVAL) version 5.8
- Common Configuration Enumeration (CCE) version 5
- Common Platform Enumeration (CPE) version 2.2
- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS) version 2.0