Certification Report

BMC ProactiveNet Performance Management 9.5

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-304-CR
Version:	1.0
Date:	12 February 2015
Pagination:	i to iii, 1 to 9

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Evaluation and Certification Scheme (CCS) – using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4*. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the CCS, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

FOREWORD

The Canadian Common Criteria Evaluation and Certification Scheme (CCS) provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the CCS Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the CCS Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of *ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories*. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is EWA-Canada.

By awarding a Common Criteria certificate, the CCS Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

This certification report is associated with the certificate of product evaluation dated 12 February 2015, and the security target identified in Section 4 of this report.

The certification report, certificate of product evaluation and security target are posted on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

This certification report makes reference to the following trademarks or registered trademarks:

- Linux is a registered trademark of Linus Torvalds Inc.;
- BMC and BMC Software are registered trademarks of BMC Software, Inc.;
- IBM and DB2 are registered trademarks of International Business Machines Corporation;
- Microsoft, Windows and Windows Server are registered trademarks of Microsoft Corporation;
- Oracle, Java and Solaris are registered trademarks of Oracle; and
- UNIX is a registered trademark of The Open Group.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

TABLE OF CONTENTS

Executive Summary

BMC ProactiveNet Performance Management 9.5 (hereafter referred to as BMC ProactiveNet), from BMC Software, Inc., is the Target of Evaluation. The results of this evaluation demonstrate that BMC ProactiveNet meets the requirements of Evaluation Assurance Level (EAL) 2 augmented for the evaluated security functionality.

BMC ProactiveNet performs real-time predictive root cause analysis to sift through events and abnormalities collected from the application and infrastructure components that support business services, identifying a prioritized set of the most likely problem causes. This information provides continuous visibility into problems as they develop; allowing the diagnosis of intermittent performance issues without requiring users to reproduce problems. BMC ProactiveNet allows users to create a baseline of the system through system monitoring. The baseline is the expected normal operating range for a metric or attribute of a monitor. Abnormalities are generated when the data values from a monitor fall outside of the normal baseline range for a statistically significant number of points within the sample window specified in the threshold. When a threshold is exceeded, BMC ProactiveNet registers this as an event. Event rules define the set of actions that can be performed when an event occurs. Event management involves setting thresholds and creating, modifying, deleting and querying event rules.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 12 February 2015 and was carried out in accordance with the rules of the Canadian Common Criteria Evaluation and Certification Scheme (CCS).

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for BMC ProactiveNet, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the CCS Certification Body, declares that the BMC ProactiveNet evaluation meets all the conditions of the *Arrangement on the Recognition of Common Criteria Certificates* and that the product will be listed on the CCS Certified Products list (CPL) and the Common Criteria portal (the official website of the Common Criteria Project).

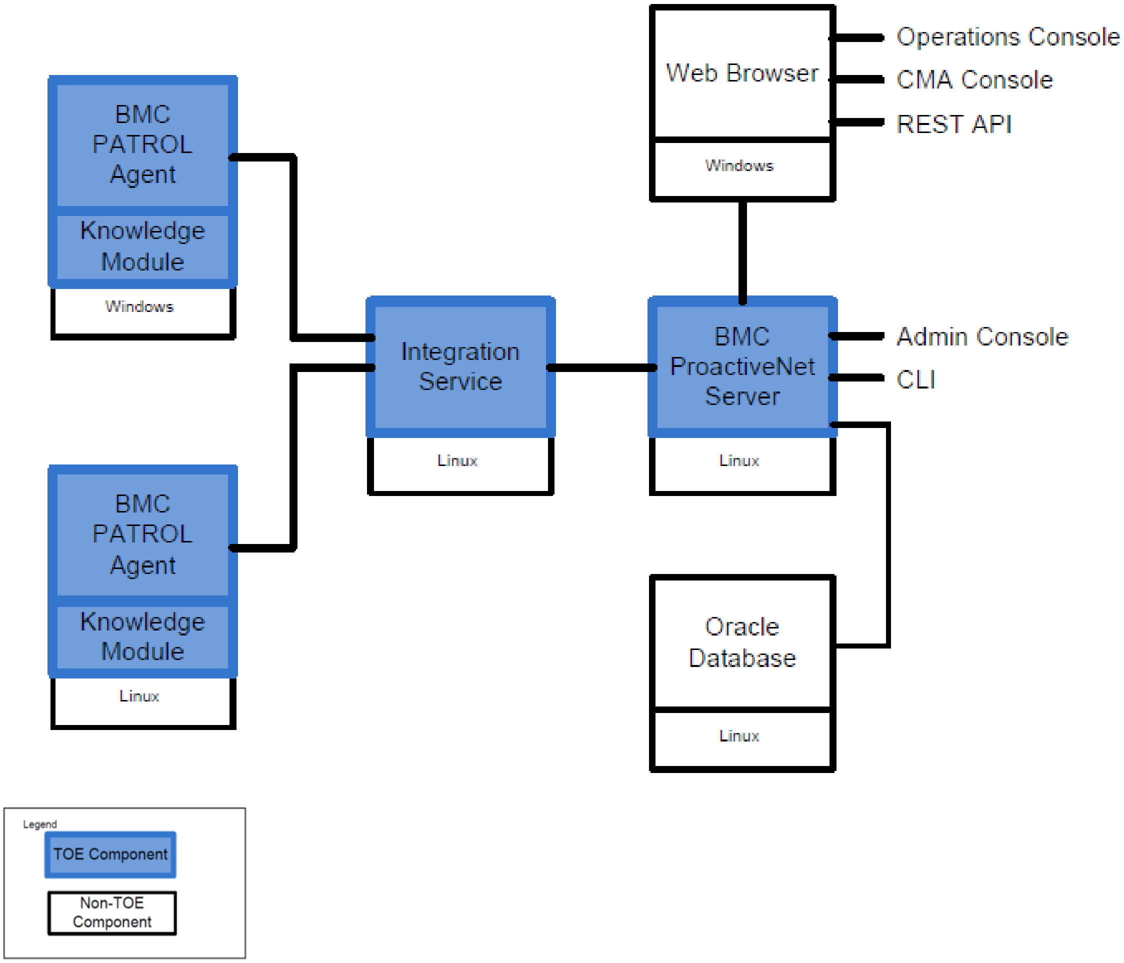
1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this EAL 2+ evaluation is BMC ProactiveNet Performance Management 9.5 (hereafter referred to as BMC ProactiveNet), from BMC Software, Inc..

2 TOE Description

BMC ProactiveNet performs real-time predictive root cause analysis to sift through events and abnormalities collected from the application and infrastructure components that support business services, identifying a prioritized set of the most likely problem causes. This information provides continuous visibility into problems as they develop; allowing the diagnosis of intermittent performance issues without requiring users to reproduce problems. BMC ProactiveNet allows users to create a baseline of the system through system monitoring. The baseline is the expected normal operating range for a metric or attribute of a monitor. Abnormalities are generated when the data values from a monitor fall outside of the normal baseline range for a statistically significant number of points within the sample window specified in the threshold. When a threshold is exceeded, BMC ProactiveNet registers this as an event. Event rules define the set of actions that can be performed when an event occurs. Event management involves setting thresholds and creating, modifying, deleting and querying event rules.

A diagram of the BMC ProactiveNet architecture is as follows:



3 Security Policy

BMC ProactiveNet implements a role-based access control policy to control administrative access to the system. In addition, BMC ProactiveNet implements policies pertaining to the following security functional classes:

- Audit;
- User Data Protection;
- Identification and Authentication;
- Security Management; and
- Performance Management.

4 Security Target

The ST associated with this Certification Report is identified below:

BMC ProactiveNet Performance Management 9.5 Security Target, v0.4, 18 July 2014.

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.*

BMC ProactiveNet is:

a. *EAL 2 augmented, containing all security assurance requirements listed, as well as the following:*

- *ALC_FLR.2 Flaw reporting procedures.*

b. *Common Criteria Part 2 extended; with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirement defined in the ST:*

- *FPM_COL_EXT Collection of Key Performance Indicators*.

c. *Common Criteria Part 3 conformant*, with security assurance requirements based only upon assurance components in Part 3.

6 Assumptions and Clarification of Scope

Consumers of BMC ProactiveNet should consider assumptions about usage and environmental settings as requirements for the product’s installation and its operating environment. This will ensure the proper and secure operation of the TOE.

6.1 Secure Usage Assumptions

The following Secure Usage Assumptions are listed in the ST:

- The operating systems upon which the TOE software runs are under the same administrative management as the TOE and is configured to restrict modification to TOE executables and configuration files to only authorized TOE Administrators.
- There will be one or more competent individuals assigned to manage the TOE. Those assigned to manage the TOE are appropriately trained and follow all administrator guidance.
- Any other systems that communicate with the TOE are under the same management control and will operate under the same security policy constraints.

6.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The computer platforms and operating systems upon which the TOE software runs operate correctly.

- The processing resources of the TOE will be located within facilities providing controlled access to prevent unauthorized physical access. Only authorized users will have physical access to the server platforms and are expected to follow all security policies.
- Only authorized TOE users and administrators will have accounts on the operating system platforms on which the TOE software executes.
- The operational environment will provide reliable system time.

7 Evaluated Configuration

The evaluated configuration for BMC ProactiveNet Performance Management 9.5 comprises:

The BMC ProactiveNet Server and BMC ProactiveNet Integration Service running Proactive Net 9.5 build 251215503 on Red Hat Enterprise Linux 6.2 (64 bit) with a BMC Patrol Agent 9.5.00i running on either a Windows 7 Professional or Red Hat Enterprise Linux 6.2 (64 bit) Operating System.

The publications entitled:

BMC PATROL Agent Reference Manual October 2010 and
BMC ProactiveNet 9.5, 18 March, 2014

describe the procedures necessary to install and operate BMC ProactiveNet in its evaluated configuration.

8 Documentation

The BMC Software, Inc. documents provided to the consumer are as follows:

- BMC PATROL Agent Reference Manual October 2010;
- BMC PATROL for Microsoft Windows Servers Getting Started Guide v9.11.10, December 2012;
- BMC PATROL for UNIX and Linux Getting Started Guide v9.11.10, December 2012; and
- BMC ProactiveNet 9.5, 18 March 2014.

9 Evaluation Analysis Activities

The evaluation analysis activities involved a structured evaluation of BMC ProactiveNet, including the following areas:

Development: The evaluators analyzed the BMC ProactiveNet functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the BMC ProactiveNet security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

Guidance Documents: The evaluators examined the BMC ProactiveNet preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the BMC ProactiveNet configuration management system and associated documentation was performed. The evaluators found that the BMC ProactiveNet configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of BMC ProactiveNet during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the BMC ProactiveNet. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the product.

All these evaluation activities resulted in **PASS** verdicts.

10 ITS Product Testing

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

10.1 Assessment of Developer Tests

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR[1].

The evaluators analyzed the developer’s test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer’s test documentation and the functional specification was complete.

10.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

[1] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Resulting from this test coverage approach is the following list of test goals:

a. Repeat of Developer's Tests: The objective of this test goal is to repeat a subset of the developer's tests;

b. Auditing of Security Management: The objective of this test goal is to confirm that roles, groups and users can be created, modified and deleted and that the actions are audited;

c. Verifying default security roles: The objective of this test goal is to confirm that permissions are assigned to users through groups;

d. Modify default values: The objective of this test goal is to confirm that an administrator can change the default values of a newly created user; and

e. Collect KPI’s (Key Performance Indicators): The objective of this test goal is to confirm that an administrator can change the default values of devices.

10.3 Independent Penetration Testing

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities;

b. Monitor for Information Leakage: The purpose of this test is to determine if the TOE is leaking any information that might be useful to an attacker; and

c. Concurrent Logins: The objective of this test goal is to confirm that concurrent logins do not cause the TOE to malfunction.

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

10.4 Conduct of Testing

BMC ProactiveNet was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The testing took place at the Information Technology Security Evaluation and Test Facility. The CCS Certification Body witnessed a portion of the independent testing. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

10.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, providing assurance that BMC ProactiveNet behaves as specified in its ST and functional specification.

11 Results of the Evaluation

This evaluation has provided the basis for an EAL 2+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

12 Evaluator Comments, Observations and Recommendations

The evaluator recommends that operators of the TOE familiarize themselves with the ST and relevant setup documentation. The operator should be aware that before installing the TOE components onto the Red Hat Enterprise Linux 6.2 (64 bit) operating system that all libraries identified in the setup documentation must be installed.

13 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CM	Configuration Management
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories - Canada
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

14 References

This section lists all documentation used as source material for this report:

a. CCS Publication #4, Technical Oversight, Version 1.8, October 2010.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.

d. BMC ProactiveNet Performance Management 9.5 Security Target, v0.4, 18 July 2014.

e. Evaluation Technical Report for BMC ProactiveNet Performance Management 9.5, v1.0, 12 February 2015.