Certification Report

EAL 4+ Evaluation of

Netezza Performance Server v4.6.5

Issued by:

Communications Security Establishment Canada

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-112-CR
Version:	1.0
Date:	10 May 2010
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, CEM, version 3.1R2, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1R2. This certification report, and its associated certificate, apply 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 Canada, 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 Canada, 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 Canada.

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 located in Ottawa, 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, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 10 May 2010, 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 and the Common Criteria Portal (the official website of the Common Criteria Project).

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

- Netezza Performance Server®
- NPS®

which are registered trademarks of the Netezza Corporation.

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

TABLE OF CONTENTS

Executive Summary

The Netezza Performance Server v4.6.5 (hereafter referred to as NPS), from Netezza Corporation, is the Target of Evaluation for this Evaluation Assurance Level (EAL) 4 augmented evaluation.

The NPS is a data warehousing product that provides support for Business Intelligence applications. The NPS system allows users to analyze data trends by processing massive amounts of data at high speed. The NPS is designed for databases ranging from approximately 2 terabytes to 100 terabytes, depending on the model chosen. By combining database, server, and storage into a single system architecture, the NPS architecture is designed to allow efficient, ad-hoc querying and analytical searches of large amounts of data at a high speed.

EWA-Canada is the CCEF that conducted the evaluation. This evaluation was completed on 14 April 2010 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 NPS, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security 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.

The results documented in the Evaluation Technical Report (ETR)[1] for this product provide sufficient evidence that it meets the EAL 4 augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM, version 3.1R2, September 2007, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1R2, September 2007. The following augmentations are claimed: e.g. ALC_FLR.3 – Systematic Flaw Remediation

NPS is conformant with the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007.

Communications Security Establishment Canada, as the CCS Certification Body, declares that NPS 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] The ETR is a CCS document that contains information proprietary to the developer and/or the evaluator, and is not releasable for public review.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented evaluation is Netezza Performance Server v4.6.5 (hereafter referred to as NPS), from Netezza Corporation.

2 TOE Description

The NPS is a data warehousing product that provides support for Business Intelligence applications. The NPS system allows users to analyze data trends by processing massive amounts of data at high speed. The NPS is designed for databases ranging from approximately 2 terabytes to 100 terabytes, depending on the model chosen. By combining database, server, and storage into a single system architecture, the NPS architecture is designed to allow efficient, ad-hoc querying and analytical searches of large amounts of data at a high speed.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for NPS is identified in Section 6 of the Security Target (ST).

4 Security Target

The ST associated with this Certification Report is identified by the following nomenclature:

Title: Netezza Corporation Netezza Performance Server v4.6.5 Security Target
Version: 0.6
Date: April 13, 2010

5 Common Criteria Conformance

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, CEM, version 3.1R2, September 2007, for conformance to the Common Criteria for Information Technology Security Evaluation, version 3.1R2, September 2007.

NPS is:

a. Common Criteria Part 2 extended, with functional requirements based upon functional components in Part 2, except for the following explicitly stated requirements defined in the ST:
   - FIT_PPC_(EXT).1, IT environment protection profile compliance,
   - FMT_MSA_(EXT).3, Static attribute initialisation,
   - FPT_TRC_(EXT).1, Internal TSF consistency, and
   - FTA_TAH_(EXT).1, TOE access history.

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3;
c. Common Criteria EAL 4 augmented, containing all security assurance requirements in the EAL 4 package, as well as the following: ALC_FLR.3 – Systematic Flaw Remediation; and
d. NPS is conformant with the U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007.

6 Security Policy

NPS implements a traditional Discretionary Access Control Policy. Users who create objects (databases, tables, etc.) are considered 'owners' of the objects which they create. Object owners have full permissions on the objects which they own. Object owners may also 'grant' permissions (full or partial) on their objects to other users or groups. The permissions for any individual user consist of a union of the permissions assigned to that user with the permissions assigned to any group of which the user is a member.

In addition, NPS implements policies pertaining to security audit, user data protection, identification and authentication, and security management. Further details on these security policies may be found in Section 6 of the ST.

7 Assumptions and Clarification of Scope

Consumers of NPS 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.

7.1 Secure Usage Assumptions

The following Secure Usage Assumption is listed in the ST:

- Personnel authorized to install, configure and operate the NPS are non-hostile, possess appropriate training and will adhere to the procedures for secure usage of the product described in the ST and the guidance documentation.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

- The NPS is installed in a physically secure location and only authorized individuals are granted physical access to the NPS.

- No general purpose computing capabilities such as compilers or user applications are installed on the NPS.

7.3 Clarification of Scope

The NPS provides a level of protection that is appropriate for basic robustness environments. It offers protection against inadvertent or casual attempts to breach security by attackers possessing an enhanced-basic attack potential. It is not intended for situations which involve determined attempts by hostile or well-funded attackers using sophisticated attack techniques.

8 Architectural Information

The NPS is composed of the following component subsystems:

a. Host;
b. Gigabit Ethernet Switch; and
c. Snippet Processing Units (SPU).

The Host component provides the central processing intelligence for the TOE, running a version of the Linux operating system. All administrative functions and external interfaces are provided by the Host. The Host receives incoming data requests and creates a query plan which is optimized to achieve the quickest possible results. The host communicates with the SPUs using the Gigabit Ethernet Switch. The SPUs are the basic unit of storage and provide query processing, data storage, and data mirroring functionality. Each SPU consists of a hard drive and a processor. Smaller NPS models include tens of SPUs while larger models may contain hundreds of SPUs, yielding many terabytes of storage. Typically multiple SPUs will be involved in processing data for a query. Each SPU will process its portion of the query independently and return the results to the Host via the Gigabit Ethernet Switch. The Host will perform final processing of the results and present them to the external interface.

9 Evaluated Configuration

The evaluated configuration for NPS comprises the following models:

a. 5200;
b. 10100a;
c. 10200a;
d. 10400a;
e. 10600a;
f. 10800a; and
g. 10050a.

The NPS software evaluated on each of the TOE models was Release 4.6.5 [Build 10670] running on Red Hat Enterprise Linux AS Version 4 Update 4.

10 Documentation

The Netezza Corporation documents provided to the consumer are as follows:

- Netezza Performance Server System Administrator's Guide, Document Number: 20282-11 Rev.3, Software Release: 4.6.5, Revised: August 18, 2009;
- Netezza Performance Server Database User's Guide, Document Number: 20284-11 Rev.3, Software Release: 4.6.5, Revised: September 3, 2009;
- Netezza Advanced Security Administrator's Guide, Document Number: D20493 Rev. 1, Software Release: 4.6.5, Revised: August 19, 2009,
- Netezza Data Loading Guide, Document Number: D20525 Rev. 1, Software Release: 4.6.5, Revised: August 19, 2009
- Netezza Performance Server ODBC, JDBC and OLE DB Installation and Configuration Guide, Document Number: 20751-11 Rev. 1, Software Release: 4.6.x, Revised: February 6, 2009,
- Netezza Performance Server Getting Started Tips, Document Number: 020293-11 Rev.1, Software Release: 4.6, Revised: February 25, 2009;
- Netezza Performance Server Release Notes, Document Number: 20283-15 Rev.3, Software Release: 4.6.5, Revised: September 8, 2009; and
- Netezza Corporation Netezza Performance Server v4.6.5 Guidance Documentation Supplement, Document Version: 0.1, September 8, 2009.

11 Evaluation Analysis Activities

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

Development: The evaluators analyzed the NPS functional specification, design documentation, and a subset of the implementation representation; they determined that the design accurately describes the TOE security functionality (TSF) interfaces and the TSF subsystems and modules, and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the NPS security architectural description and determined that the initialization process was secure and that the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance Documents: The evaluators examined the NPS preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously described 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 were complete and sufficiently detailed to result in a secure configuration.

Life-cycle support: An analysis of the NPS configuration management system and associated documentation was performed. The evaluators found that the NPS configuration items were clearly marked and could be modified and controlled by automated tools. The developer’s configuration management system was observed during a site visit, and it was found to be mature and well-developed and operated in accordance with the CM plan. The evaluators confirmed that the access control measures as described in the CM plan are effective in preventing unauthorized access to the configuration items.

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

The evaluators examined the development security procedures during a site visit and determined that they detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the NPS design and implementation. The evaluators determined that the developer has used a documented model of the TOE life-cycle and well-defined development tools that yield consistent and predictable results.

The evaluators reviewed the flaw remediation procedures used by Netezza Corporation for NPS. 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.

Vulnerability Assessment: The evaluators conducted an independent vulnerability analysis of NPS. Additionally, the evaluators conducted a review of public domain vulnerability databases and a focused search of all evaluation deliverables. The evaluators identified potential vulnerabilities for testing applicable to the NPS in its operational environment.

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

12 ITS Product Testing

Testing at EAL 4 consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

12.1 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[2].

The evaluators analyzed the developer's test coverage and depth analysis and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification, TOE design and security architecture description was complete.

12.2 Independent Functional Testing

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation, examining the developer's test documentation, executing a sample of the developer's test cases, and creating test cases that augmented the developer tests.

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 was the following list of EWA-Canada 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. Initialization: The objective of this test goal is to provide the procedures for determining the system configuration in order to ensure that the TOE that is tested is correct;

c. Identification and Authentication: The objective of this test goal is to ensure that the identification and authentication requirements have been met;

d. Audit: The objective of this test goal is to ensure that the audit data is recorded and can be viewed; and

e. Security Management: The objective of this test goal is to ensure the functionality around creating, managing and deleting users and groups is correct.

12.3 Independent Penetration Testing

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

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

a. Generic vulnerabilities;
b. Bypassing;
c. Tampering; and
d. Direct attacks.

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

12.4 Conduct of Testing

NPS 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 (ITSET) Facility at EWA-Canada. Testing for the NPS was tested on one model of the hardware that was physically located in the ITSET Facility and two models were tested remotely, as they were physically located in the Netezza 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.

12.5 Testing Results

The developer’s tests and the independent functional tests yielded the expected results, giving assurance that NPS behaves as specified in its ST, functional specification, TOE design and security architecture description.

13 Results of the Evaluation

This evaluation has provided the basis for an EAL 4+ level of assurance. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

14 Evaluator Comments, Observations and Recommendations

In all cases, the TOE is installed and configured by Netezza personnel. Upgrades to the product are also performed by Netezza personnel.

The user documentation for the NPS describes in detail the discretionary access control policy implemented by the TOE as well as the extensive logging and auditing features of the product. The developer has produced a guidance supplement which includes specific instructions applicable to the evaluated configuration of the product.

15 Acronyms, Abbreviations and Initializations

Acronym/Abbreviation/ Initialization	Description

Acronym/Abbreviation/ Initialization	Description
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
CPL	Certified Products list
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
NPS	Netezza Performance Server
PALCAN	Program for the Accreditation of Laboratories - Canada
SPU	Snippet Processing Unit
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality

16 References

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

a. CCS Publication #4, Technical Oversight, Version 1.1, August 2005.

b. Common Criteria for Information Technology Security Evaluation, Version 3.1 R2, September 2007.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 R2, September 2007.

d. U.S. Government Protection Profile for Database Management Systems in Basic Robustness Environments, Version 1.2, July 25, 2007.

e. Netezza Corporation Netezza Performance Server v4.6.5 Security Target, 0.6, April 13, 2010.

f. Evaluation Technical Report for EAL 4+ Common Criteria Evaluation of Netezza Corporation Netezza Performance Server, v4.6.5, Version 1.7, 14 April 2010