Certification Report

EAL 3+ Evaluation of

Netezza Performance Server® Version 3.0

Issued by:

Communications Security Establishment

Certification Body

Canadian Common Criteria Evaluation and Certification Scheme

Document number:	383-4-59-CR
Version:	1.0
Date:	17 September 2007
Pagination:	i to iv, 1 to 11

DISCLAIMER

The Information Technology (IT) product identified in this certification report, and its associated certificate, have 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 2.3*, for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3*. 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 (CSE), 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 CSE, 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 (CSE).

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 Standard 17025, General requirements for the accreditation of calibration and testing 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 Electronic Warfare Associates-Canada, Ltd. located in Ottawa, Ontario.

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 17 September 2007, 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 at: http://www.cse-cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official Common Criteria Program website at http://www.commoncriteriaportal.org/

This certification report makes reference to the following trademarked names:

- Netezza Performance Server®
- NPS®

which are registered trademarks of the Netezza Corporation.

TABLE OF CONTENTS

Executive Summary

The Netezza Preformance Server®, from Netezza Corporation, (hereafter referred to as NPS®) is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 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.

Electronic Warfare Associates-Canada, Ltd. is the Common Criteria Evaluation Facility that conducted the evaluation. This evaluation was completed on 4 September 2007 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 the NPS®, the security requirements, and the level of confidence (evaluation assurance level) at which the product is intended to satisfy the security requirements. Consumers of the NPS® are advised to verify that their operating environment is consistent with 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 3 Augmented assurance requirements for the evaluated security functionality. The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3* (with applicable final interpretations), for conformance to the *Common Criteria for Information Technology Security Evaluation, version 2.3*. The following augmentation is claimed:

ALC_FLR.2 – Flaw reporting procedures.

CSE, as the CCS Certification Body, declares that the 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) at http://www.cse-

[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.

cst.gc.ca/services/common-criteria/trusted-products-e.html and on the official International Common Criteria Program website at http://www.commoncriteriaportal.org.

1 Identification of Target of Evaluation

The Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 3 augmented evaluation is the Netezza Performance Server® Version 3.0, from Netezza Corporation, (hereafter referred to as NPS®).

2 TOE Description

The NPS® is a database appliance that integrates a database, server, and storage into a single system architecture. The NPS® architecture is designed to allow efficient, ad-hoc querying of large amounts of data at high speed. In a typical deployment of the NPS®, data is placed into the NPS® from a corporate data source (e.g. an e-commerce transactional database, a corporate customer information database, or a corporate wide data collection system). End users of the product access this data through a custom Business Intelligence application. This Business Intelligence application provides the user with mechanisms to perform queries and analysis on sets of data. The Business Intelligence application accesses the NPS® appliance on behalf of the user through standard ODBC (Open Database Connectivity) or JDBC (Java Database Connectivity) interfaces to submit SQL queries to the NPS®. The NPS® identifies and authenticates all database users and implements a traditional discretionary access control mechanism in order to control access to specific data. The NPS® provides extensive logging and audit capabilities.

3 Evaluated Security Functionality

The complete list of evaluated security functionality for the NPS® is identified in Section 5 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® version 3.0, Netezza Security Target
Version: 1.1
Date: 04 September 2007

5 Common Criteria Conformance

The evaluation was conducted using the *Common Methodology for Information Technology Security Evaluation, Version 2.3*, for conformance to the *Common Criteria for Information Technology Security Evaluation, Version 2.3*. The NPS® is:

a. Common Criteria Part 2 conformant, with security functional requirements based only upon functional components in Part 2;

b. Common Criteria Part 3 conformant, with security assurance requirements based only upon assurance components in Part 3; and

c. Common Criteria EAL 3 Augmented, with all the security assurance requirements in EAL 3, as well as ALC_FLR.2 - Flaw reporting procedures.

6 Security Policy

The TOE 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, the 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 5 of the ST.

7 Assumptions and Clarification of Scope

Consumers of the NPS® product 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 assumptions are listed in the ST:

a. 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.

7.2 Environmental Assumptions

The following Environmental Assumptions are listed in the ST:

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

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

For more information about the TOE security environment, refer to Section 3 of the ST (TOE Security Environment).

7.3 Clarification of Scope

The NPS® provides a level of protection that is appropriate for low robustness environments processing unclassified information. It offers protection against inadvertent or casual attempts to breach system security, by unsophisticated attackers possessing a low 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 Snippet Processing Units (SPU) 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 NPS® Security Target defines the following evaluated configurations of the TOE:
a. 5200;
b. 8050z;
c. 8150z;
d. 8250z;
e. 8450z; and
f. 8650z.

The NPS® software evaluated on each of the TOE models was Release 3.0.6 [Build 6414] running on Red Hat Enterprise Linux AS (Intel 32-bit) Version 4.

10 Documentation

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

a. Netezza Performance Server Administrator’s Guide, Document Number: 20282-6 Rev. 1, Software Release: 3.0, Revised: 18 November 2005;

b. Netezza Performance Server Database User's Guide, Document Number: 20284-6 Rev. 1, Software Release: 3.0, Revised: 18 November 2005;

c. Netezza Performance Server Getting Started Tips, Document Number: 020293-6 Rev. 1, Software Release: 3.0; and

d. Netezza Corporation, Netezza Performance Server 3.0, AGD & IGS Readme, Document Version 0.2, 11 May 2007.

11 Evaluation Analysis Activities

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

Configuration management: An analysis of the NPS® development environment and associated documentation was performed. The evaluators found that the NPS® configuration items were clearly marked, and could be modified and controlled. The developer's configuration management system was observed during a site visit, and it was found to be mature and well developed.

Secure delivery and operation: The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the NPS® during distribution to the consumer. The evaluators examined and tested the installation, generation and start-up procedures, and determined that they were complete and sufficiently detailed to result in a secure configuration.

Design documentation: The evaluators analysed the NPS® functional specification and high-level design; they determined that the documents were internally consistent, and completely and accurately instantiated all interfaces and security functions. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

Guidance documents: The evaluators examined the NPS® user and administrator guidance documentation and determined that it sufficiently and unambiguously described how to securely use and administer the product, and that it was consistent with the other documents supplied for evaluation.

Life-cycle support: The evaluators assessed 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 documented flaw remediation process was carefully reviewed, demonstrating that adequate procedures are in place to track and correct security flaws, and distribute the flaw information and corrections.

Vulnerability assessment: The strength of function claim from the Security Target of the NPS® was validated through independent evaluator analysis. The evaluators also validated the developer's vulnerability analysis and found that it sufficiently described each of the potential vulnerabilities along with a sound rationale as to why it was not exploitable in the intended environment. In addition, the evaluators analyzed the guidance documentation for any ambiguities that could lead to an insecure configuration, performed an independent vulnerability analysis and developed tests that focused on potential vulnerabilities in the NPS®.

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

12 ITS Product Testing

Testing at EAL 3 consists of the following three steps: assessing developer tests in terms of coverage and depth, performing independent functional tests, and performing independent penetration tests.

12.1 Assessing Developer Tests

The evaluator assessed NPS® test documentation for both coverage and depth. The testing effort included multiple tests for each of the security functions provided by the product and exercised all of the security relevant functionality of each of the externally visible TOE interfaces. In selecting a subset of the developer's tests for repetition during the evaluation, the evaluators selected a sample of approximately 30% of the developer's tests. Tests were selected across the entire range of product security functionality and included at least one test procedure for each of the security functions claimed by the TOE.

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. The following areas were tested:

a. Product Initialization;
b. Identification and Authentication;
c. Security Audit;
d. Security Management; and
e. User Data Protection.

12.3 Independent Penetration Testing

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

- Generic vulnerabilities;

- Bypassing;
- Tampering; and
- Direct Attacks.

The evaluator conducted a port scan of the NPS®. Only the ports listed in the installation instructions were found to be open. The evaluator used a publicly available tool to scan the NPS® for generic vulnerabilities, and none were found. In addition, the evaluator performed direct attacks on the NPS®, attempting to bypass or break the TOE's discretionary access control security mechanisms.

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

12.4 Conduct of Testing

The NPS® was subjected to a comprehensive suite of formally documented, independent functional tests. The testing took place at the Information Technology Security Evaluation and Test (ITSET) Facility at Electronic Warfare Associates-Canada, Ltd. and at the developer's facility in Framingham, MA. 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 the Evaluation Technical Report (ETR)[2].

12.5 Testing Results

The developer's tests and the independent functional tests yielded the expected results, giving assurance that the NPS® behaves as specified in its ST and functional specification. The penetration testing resulted a PASS verdict, as the evaluators were unable to exploit any of the identified potential vulnerabilities in the NPS® in its intended operating environment.

13 Results of the Evaluation

This evaluation has provided the basis for an **EAL 3+** 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.

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

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
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CPL	Certified Products list
CSE	Communications Security Establishment
DAC	Discretionary Access Control
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
JDBC	Java Database Connectivity
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
ODBC	Open Database Connectivity
PALCAN	Program for the Accreditation of Laboratories Canada
SFP	Security Function Policy
SPU	Snippet Processing Unit
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

16 References

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

a. Canadian Common Criteria Evaluation and Certification Scheme (CCS) and CCS Publication #4, Technical Oversight, Version 1.0.

b. Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005.

c. Common Methodology for Information Technology Security Evaluation, CEM, Version 2.3, August 2005.

d. Netezza Corporation, Netezza Performance Server® version 3.0, Netezza Security Target, Document Version 1.1, 4 September 2007.

e. Evaluation Technical Report (ETR) Netezza Performance Server®, EAL 3+ Evaluation, Common Criteria Evaluation Number: 383-4-59, Document No. 1537-000-D002, Version 1.0, 4 September 2007.