Common Criteria Certification Report

Dell PowerProtect Data Manager v19.22

CAN-675-LSS

14 July 2026

v1.0

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité
Canada

Foreword

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE).

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security (a branch of CSE). 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 Canadian Common Criteria Program, and the conclusions of the testing laboratory 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 Canadian Centre for Cyber Security, 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 Canadian Centre for Cyber Security, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your organization has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

Canadian Centre for Cyber Security

Contact Centre and Information Services

contact@cyber.gc.ca | 1-833-CYBER-88 (1-833-292-3788)

Overview

The Canadian Common Criteria Program provides a third-party evaluation service for evaluating the security of IT products. Evaluations are performed by a commercial Common Criteria Testing Laboratory (CCTL) under the oversight of the Certification Body, which is managed by the Canadian Centre for Cyber Security.

A CCTL is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target (ST). 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 ST, in addition to this certification report, 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 CCTL.

The certification report, certificate of product evaluation and ST are posted to the Common Criteria portal (the official website of the International Common Criteria Program).

TABLE OF CONTENTS

Executive Summary CAN-675-LSS

Dell PowerProtect Data Manager v19.22 (hereafter referred to as the Target of Evaluation, or TOE), from **Dell Technologies** , was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that the TOE meets the following conformance claim: **EAL 2+ ALC_FLR.2**

Lightship Security is the CCTL that conducted the evaluation. This evaluation was completed on **14 July 2026** and was conducted in accordance with the rules of the Canadian Common Criteria Program.

The scope of the evaluation is defined by the Security Target, which identifies assumptions made during the evaluation, the intended environment for the TOE, 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 consider the comments, observations, and recommendations in this Certification Report.

The Canadian Centre for Cyber Security, as the Certification Body, declares that this evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product is listed on the Certified Products list for the Canadian Common Criteria Program and the Common Criteria portal (the official website of the International Common Criteria Program).

Identification of Target of Evaluation

The Target of Evaluation (TOE) is identified as follows:

Table 1: TOE Identification

TOE Name and Version	Dell PowerProtect Data Manager v19.22
Developer	Dell Technologies

See the Evaluated Configuration section for more details on the evaluated configuration of the TOE.

Common Criteria Conformance

The evaluation was conducted using the following methodology:

Common Methodology for Information Technology Security Evaluation, 2022 Release 1, for conformance to the Common Criteria for Information Technology Security Evaluation, 2022 Release 1

The TOE claims the following conformance:

EAL 2+ ALC_FLR.2

TOE Description

The TOE is a virtual appliance that allows administrators to provision data paths between asset sources and storage targets, enabling users to initiate backup and restore operations on user data. Administrators can create protection policies to automate, schedule, and monitor backups for VMware virtual machines.

Self-service users can perform on-demand backup and restore operations using a Web GUI or REST API. Administrators can manage the TOE using the Web GUI and REST API.

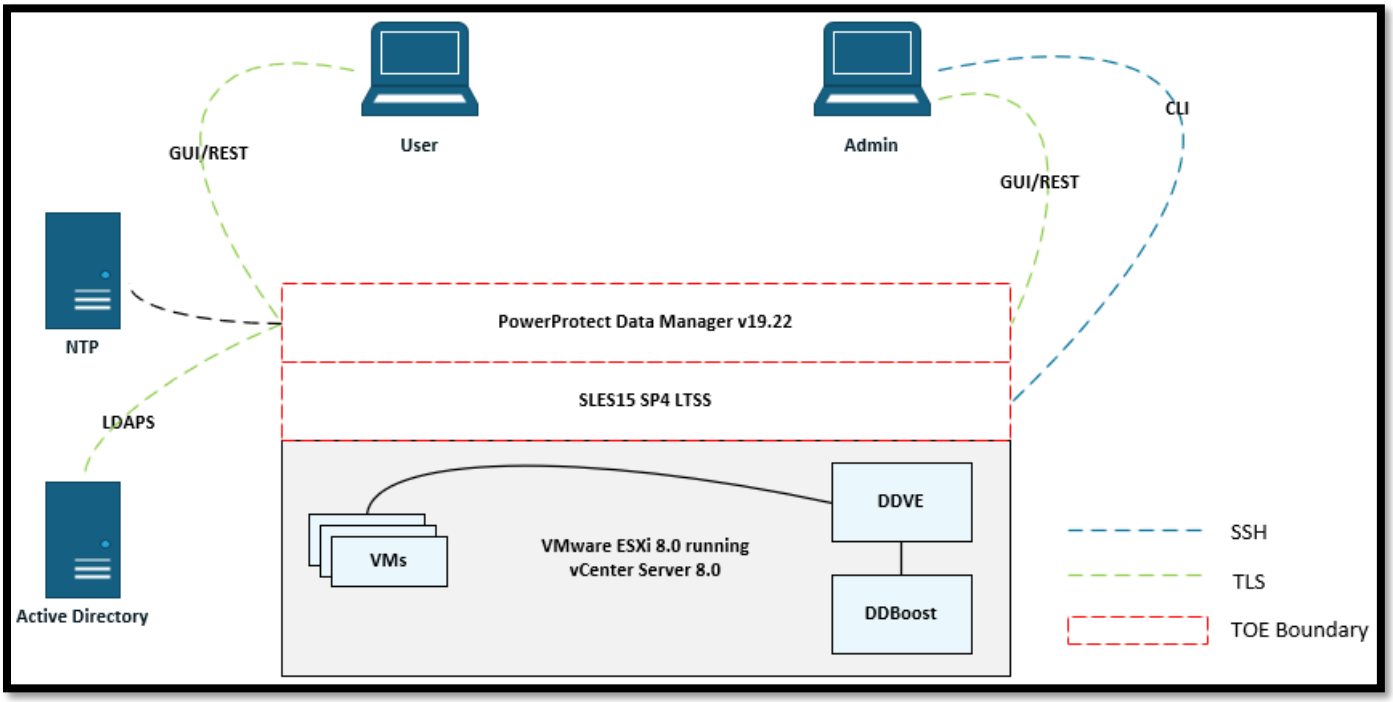

Figure 1: TOE Architecture

Security Policy

The TOE implements and enforces policies pertaining to the following security functionality:

- Security Audit
- Identification and Authentication
- Trusted Path
- User Data Protection
- Security Management

Complete details of the security functional requirements (SFRs) can be found in the Security Target.

Assumptions and Clarification of Scope

Consumers of the TOE 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.

Usage and Environmental Assumptions

The following assumptions are made regarding the use and deployment of the TOE:

- The TOE will be located within controlled access facilities, which will prevent unauthorized physical and logical access.
- There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
- The TOE will rely on external storage for maintaining backup and recovery data.
- The TOE will rely on the operational environment for reliable time.
- Non-administrative users of the TOE are trusted and follow all guidance.

Clarification of Scope

The following features are excluded from this evaluation:

- Log offloading
- SupportAssist
- Data Deduplication and Data Replication provided by DDVE and DD Boost

The following asset types are also supported by the TOE but are excluded from this evaluation:

- File Systems
- Kubernetes Clusters
- MS Exchange Server and SQL Server Databases
- Oracle Databases
- SAP HANA Databases
- Network-Attached Storage (NAS) Shares
- PowerStore, PowerMax, and VMAX Storage

Evaluated Configuration

The evaluated configuration for the TOE comprises:

Table 2: Evaluated Configuration

TOE Software/Firmware	PowerProtect Data Manager v19.22 build 19.22.0-24 packaged with SLES15 SP4 Operating System.
Environmental Support	VMware ESXi with vCentre Server 8.0, Active Directory Server, NTP Server, DDVE 8.3, DD Boost 8.6.

Documentation

The following documents are available to the consumer to assist in the configuration and installation of the TOE:

a) PowerProtect Data Manager 19.22 Administrator Guide, February 2026, Rev.02
b) PowerProtect Data Manager 19.22 Deployment Guide, February 2026, Rev.02
c) PowerProtect Data Manager 19.22 Security Configuration Guide, November 2025, Rev. 01
d) PowerProtect Data Manager 19.22 VMware Virtual Machine User Guide, November 2025, Rev. 01
e) PowerProtect Data Manager (V19.22.0) REST API
f) Dell PowerProtect Data Manager v19.22 Common Criteria Guide, Version 1.7

Evaluation Analysis Activities

The evaluation activities comprised a structured assessment of the TOE. Documentation and processes related to Development, Guidance Documentation, and Life-Cycle Support were reviewed and analyzed.

Development

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements. The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

Guidance Documents

The evaluators examined the TOE 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 exercised 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 TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

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

The developer's flaw remediation procedures were reviewed and found to be effective in tracking and correcting identified flaws, as well as in distributing flaw-related information and corrective updates.

Testing Activities

Testing consists of the following three steps: assessing developer tests, performing independent tests, and performing a vulnerability analysis.

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 Evaluation Test Report (ETR). The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

Conduct of Testing

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate proprietary test results document.

Independent Testing

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

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developer's tests;
b. HTTPS Proxy Testing: The evaluator verified whether the WebUI and the REST API can use the same interface;
c. Concurrent REST API: The evaluator confirmed the separation of roles with concurrent users using the REST interface;
d. Direct Use of WebUI by REST Client: The evaluator attempted to use the WebUI as a non administrator user and verified correct access control was enforced;
e. Separation of LDAP group membership: The evaluator assigned an LDAP user to multiple groups to verify the TOE provides access based on group membership;
f. Asset Group Access: The evaluator verified that different asset groups limit access based on roles;
g. Reset OS passwords via REST API: Using a proxy the evaluator attempted to reset OS passwords as a user without permissions;

h. Reset asset passwords via REST API: Using a proxy the evaluator attempted to reset asset as a user without permissions; and

i. Interoperability Testing: Using a known good implementation the evaluator confirmed that the TOE uses the claimed cipher suites for SSH and TLS connections.

Independent Testing Results

The testing produced the expected results, supporting the conclusion that the TOE correctly implements the functional requirements specified in the ST and the TOE functional specification.

Vulnerability Analysis

The evaluators conducted an independent review of all evaluation evidence, public domain vulnerability databases, and technical community sources. Additionally, the evaluators used automated vulnerability scanning tools to discover potential network, platform, and application layer vulnerabilities. Based upon this review, the evaluators formulated flaw hypotheses , which they used in their vulnerability analysis.

Public domain searches were conducted on **13 May 2026** and included the following search terms:

Power Protect Data Manager	PPDM	Suse Linux Enterprise Server 15 SP4
OpenSSL 1.1.1l	NGINX 1.26.3	ESXi 8.0
DD Boost	OpenSSH 8.4p1	

The evaluator also used a Software Bill Of Materials during the public domain search.

Vulnerability searches were conducted using the following sources:

Dell security advisories https://www.dell.com/support/security/en-au	NIST National Vulnerabilities Database https://web.nvd.nist.gov/view/vuln/search
CISA - Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog	CCCS – Alerts and advisories https://cyber.gc.ca/en/alerts-advisories

Vulnerability Analysis Results

The vulnerability analysis did not uncover any security relevant residual exploitable vulnerabilities in the intended operating environment.

Results of the Evaluation

The Information Technology product identified in this certification report, and its associated certificate, has been evaluated at an approved testing laboratory established under the Canadian Centre for Cyber Security. This certification report, and its associated certificate, apply only to the specific version and release of the product in its evaluated configuration.

The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

Recommendations/Comments

It is recommended that all guidance be followed to configure the TOE in the evaluated configuration.

Supporting Content

List of Abbreviations

Term	Definition
ACVP	Automated Cryptographic Validation Protocol
CAVP	Cryptographic Algorithm Validation Program
CCTL	Common Criteria Testing Laboratory
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ESV	Entropy Source Validation
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

References

Reference
Common Criteria for Information Technology Security Evaluation, 2022 Release 1.
Common Methodology for Information Technology Security Evaluation, CEM, 2022 Release 1.
Dell PowerProtect Data Manager v19.22 Security Target, v1.8, July 13, 2026.
Dell PowerProtect Data Manager v19.22 Evaluation Technical Report, July 14, 2026.