Veritas NetBackup™ 8.2

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2126-000-D102
Version: 1.2
27 February 2020

Veritas Technologies
2625 Augustine Drive,
Santa Clara, California
95054

Prepared by:
EWA-Canada, An Intertek Company
1223 Michael Street North, Suite 200
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the Target of Evaluation (TOE), the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target reference, the Target of Evaluation reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria and Packages. The ST does not conform to a Protection Profile.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the IT environment.

Section 7, TOE Summary Specification, describes the security functions that are included in the TOE to enable it to meet the IT security functional requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Veritas NetBackup™ 8.2 Security Target
ST Version:	1.2
ST Date:	27 February 2020

1.3 TOE REFERENCE

TOE Identification:	Veritas NetBackup™ 8.2 and NetBackup 5240 Appliance Release 3. 2
TOE Developer:	Veritas Technologies
TOE Type:	Backup and Recovery (Other Devices and Systems)

1.4 TOE OVERVIEW

Veritas NetBackup is an Enterprise data backup and recovery solution. It provides cross-platform backup functionality for a variety of Windows and Linux operating systems.

NetBackup administrators can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. An administrator can carefully schedule backups to achieve systematic and complete backups over a period of time, and optimize network traffic during off-peak hours.

NetBackup includes both the server and the client software as follows:

- Server software resides on the computers that manage the storage devices
- Client software resides on computers that contain the data that is backed up

NetBackup accommodates multiple servers that work together under the administrative control of one NetBackup Master Server in the following ways:

- The Master Server manages backups, archives, and restores, and is responsible for media and device selection for NetBackup. The Master Server contains the NetBackup catalog. The catalog contains the internal databases that contain information about NetBackup backups and configuration.
- Media Servers provide additional storage by allowing NetBackup to use the storage devices that are attached to them. Media Servers can also increase performance by distributing the network load.

During a backup, the client sends backup data across the network to a NetBackup server. The NetBackup server manages the type of storage that is specified in the backup policy, and ensures that the backup data is encrypted for storage. During a restore, administrators can browse, and then select the files and directories to recover. NetBackup finds the selected files and directories and restores them to the disk on the client system.

Major security features include:

- Backup and recovery of user data
- Encryption of backup data using Federal Information Processing Standards (FIPS)-validated cryptography

- Secure, role-based administration with access control
- Audit generation and reviewing functions

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following operating system and hardware components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Master Server machine	Red Hat Enterprise Linux (RHEL) 7.6	General Purpose Computer Hardware
Media Server machine	Windows Server 2012 R2	General Purpose Computer Hardware
Linux Client	RHEL 7.6	General Purpose Computer Hardware
Windows Client	Windows Server 2012 R2	General Purpose Computer Hardware

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

The TOE includes both the NetBackup software and the NetBackup appliance, and the claimed security functionality applies to both implementation types. Unless otherwise indicated, the descriptions of how the security claims are met apply to both the software and the appliance.

1.5.1 Physical Scope

The TOE is made up of a Master Server, a Media server, a Media Server appliance, and clients on Windows 2012 and RHEL 7.6. The components are described in Table 2 and depicted in Figure 1.

Component	Description
Master Server	Veritas NetBackup 8.2 software
Media Server	Veritas NetBackup 8.2 software
Media Server Appliance	NetBackup 5240 Appliance, version 3.2[1]
Linux Client	Veritas NetBackup 8.2 software for RHEL 7.6
Windows Client	Veritas NetBackup 8.2 software for Windows Server 2012

Table 2 –TOE Components

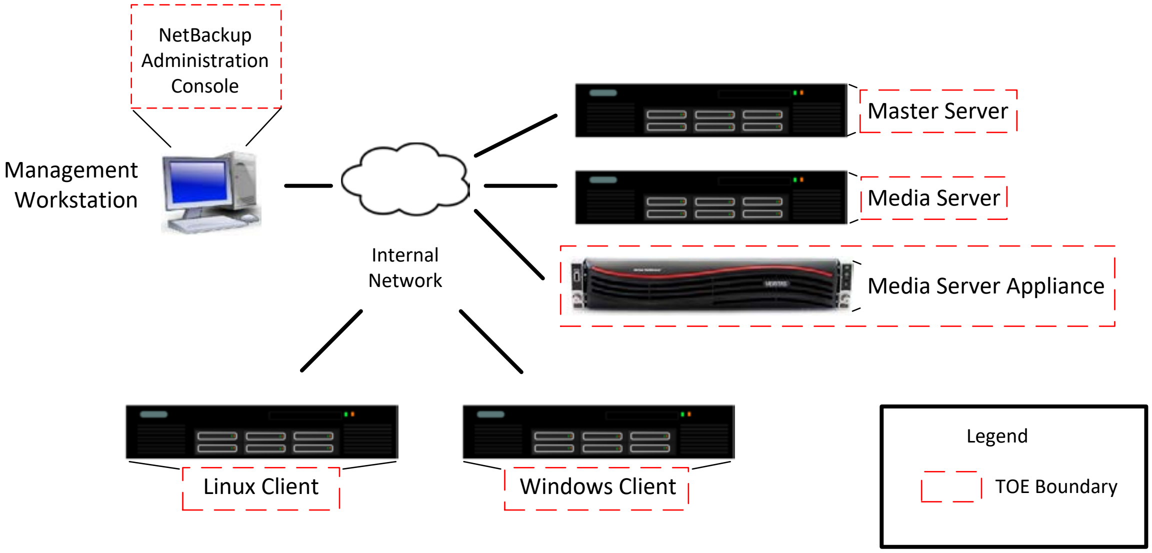

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The evaluated configuration consists of the Master Server on Red Hat Linux, the Media Service installed on Windows, a Media Server Appliance, a Red Hat Linux Client and a Windows client.

The following packages include the Master Server, Media Server and Client. Customers can download the TOE software from the Veritas Entitlement Management System using the following files:

- For Red Hat Linux:
  - NetBackup_8.2_LinuxR_x86_64.tar.gz

[1] Version 3.2 of the NetBackup Appliance includes NetBackup 8.2 software.

- For Windows:
  - Windows – NetBackup_8.2_Win.zip

This file provides the software for the Master Server, Media Server and agents.

The NetBackup appliance is delivered by a trusted courier, such as FedEx.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation:

- Veritas NetBackup™ Administrator's Guide, Volume I, UNIX, Windows, and Linux, Release 8. 2, Last updated: 2019-07-01
  - NetBackup82_AdminGuideI_Server.pdf
- Veritas NetBackup™ Security and Encryption Guide, UNIX, Windows, and Linux, Release 8. 2, Last updated: 2019-06-28
  - NetBackup82_Security_and_Encryption_Guide.pdf
- NetBackup™ Web UI Security Administrator's Guide Release 8. 2, Last updated: 2019-06-28
  - NetBackup82_WebUIGuide_SecurityAdmin.pdf
- Veritas Appliance Management Guide NetBackup Appliance 3.2 (AMS 1.3)
  - Appliance Management Guide_32.pdf
- Veritas NetBackup™ 52xx Appliance Initial Configuration Guide Release 3.2
  - NetBackup 52xx Appliance Initial Configuration Guide - 32.pdf
- Veritas NetBackup™ Appliance Security Guide Release 3.2, 2019
  - NetBackup Appliance Security Guide - 32.pdf
- Veritas NetBackup™ Installation Guide UNIX and Windows Release 8.2
  - NetBackup82_InstallGuide.pdf
- NetBackup™ Web UI Backup Administrator's Guide Release 8.2
  - NetBackup82_WebUIGuide_BackupAdmin.pdf
- Veritas NetBackup™ Commands Reference Guide UNIX, Windows, and Linux Release 8.2
  - NetBackup82_Commands.pdf
- Veritas NetBackup™ Status Codes Reference Guide UNIX, Windows, and Linux Release 8.2
  - NetBackup82_RefGuide_StatusCodes.pdf
- Veritas NetBackup™ 8.2 Common Criteria Guidance Supplement, Version 0.1
  - Veritas_NetBackup_EAL2_AGD_01.pdf

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 3 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events, and include the identity of the user that initiated the recorded event. The audit logs may be filtered for review by authorized administrators.
Cryptographic Support	Cryptographic functionality is provided to encrypt backup data.
User Data Protection	The TOE provides backup and recovery functionality. The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE.
Identification and Authentication	The TOE ensures that users are identified and authenticated prior to being granted access to TOE functions. Passwords are obscured as they are entered.
Security Management	The TOE provides management capabilities via a Web-Based User Interface (UI), a Command Line Interface (CLI) and the NetBackup Administration Console. Management functions allow the administrators to configure users and roles, and manage backup and recovery functionality.
Protection of the TSF[2]	Reliable timestamps are provided for inclusion in audit records.

Table 3 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

The Master Server and Media Server can be installed on Linux or Windows, or the NetBackup appliance. Although there are many installation options, the evaluated configuration is limited to the Master Server on RHEL 7.6, one Media Server on Windows Server 2012 and a Media Server Appliance.

The descriptions of Role Based Access Control refer to Root users, since the Master Server is installed on RHEL. These access controls would apply equally to Windows Administrators where the Master Server is installed on a Windows

[2] TOE Security Functionality

Server. However, this functionality was not assessed in the evaluated configuration.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 has been taken into account.

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

This ST does not claim conformance of the TOE with any Protection Profile (PP).

2.3 PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2 Flaw Reporting Procedures.

2.4 CONFORMANCE RATIONALE

This ST does not claim conformance of the TOE with any PP, therefore a conformance rationale is not applicable.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 4 lists the threats addressed by the TOE. The threat agents to the TOE are considered to be unauthorized users with public knowledge of how the TOE operates and who possess the skills and resources to alter TOE configuration settings, or parameters, or both. The threat agents do not have physical access to the TOE.

Mitigation of the threats is through the objectives identified in Section 4.1, Security Objectives for the TOE.

Threat	Description
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.
T.PRIVILEGE	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
T.UNAUTH	An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.

Table 4 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 5 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ACCOUNT	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
P.MANAGE	The TOE shall be managed only by authorized users.

Table 5 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 6.

Assumptions	Description
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These users are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.
A.NETWORK	The TOE components and their hosts are installed on an internal network which protects the data from disclosure and modification by untrusted systems or users.
A.PROTECT	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical access.

Table 6 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE, and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.
O.AUDIT	The TOE must generate audit records for security related events.
O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
O.CRYPTO	Backup data must be protected using approved cryptographic functions.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
O.PROTECT	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.
O.TIME	The TOE must provide reliable timestamps.

Table 7 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by the IT environment or by non-technical or procedural means.

Security Objective	Description
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
OE.NETWORK	The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 8 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organizational policies identified for the TOE.

	T.IMPCON	T.PRIVILEGE	T.UNAUTH	P.ACCOUNT	P.BACKUP	P.MANAGE	A.MANAGE	A.NETWORK	A.PROTECT
O.ACCESS	X	X	X			X			
O.ADMIN	X					X			
O.AUDIT	X		X	X					
O.BACKUP					X				
O.CRYPTO			X						
O.IDENTAUTH	X	X		X		X			
O.PROTECT		X				X			
O.TIME				X					
OE.INSTALL	X					X	X		
OE.NETWORK								X	
OE.PERSON						X	X		

	T.IMPCON	T.PRIVILEGE	T.UNAUTH	P.ACCOUNT	P.BACKUP	P.MANAGE	A.MANAGE	A.NETWORK	A.PROTECT
OE.PHYSICAL							X		X

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE.

Threat: **T.IMPCON**	An unauthorized user may inappropriately change the configuration of the TOE causing potential unauthorized data accesses to go undetected.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.
	O.AUDIT	The TOE must generate audit records for security related events.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
Rationale:	The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.ADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions. The O.ACCESS objective builds upon the O.IDENTAUTH objective by only permitting authorized users to access TOE functions. The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access	

	attempts.

Threat: **T.PRIVILEGE**	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTECT	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.
Rationale:	The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions. The O.ACCESS objective builds upon the O.IDENTAUTH objective by permitting only authorized users to access TOE functions. The O.PROTECT objective addresses the threat by providing self-protection for the TOE.	

Threat: **T.UNAUTH**	An unauthorized user may attempt to access backup data which could result in the loss of sensitive information.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.AUDIT	The TOE must generate audit records for security related events.
	O.CRYPTO	Backup data must be protected using approved cryptographic functions.
Rationale:	The O.ACCESS objective permits only authorized access to TOE data. The O.AUDIT objective supports O.ACCESS by requiring the TOE to record audit data for security related events such as unauthorized access attempts. The O.CRYPTO objective ensures that user data is protected from disclosure in the case of attempted data access.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE.

Policy: **P.ACCOUNT**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.AUDIT	The TOE must generate audit records for security related events.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	The O.AUDIT objective requires auditing of all data access and use of TOE functions. The O.TIME objective supports this policy by providing a time stamp for insertion into the resulting audit records. The O.IDENTAUTH objective supports this policy by ensuring each user is uniquely identified and authenticated.	

Policy: **P.BACKUP**	The TOE shall backup specified client data and make it available for restore operations.	
Objectives:	O.BACKUP	The TOE shall backup specified client data and make it available for restore operations.
Rationale:	The O.BACKUP objective requires the TOE to backup specified client data, and requires the TOE to make that data available for restore operations.	

Policy: **P.MANAGE**	The TOE shall be managed only by authorized users.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.
	O.PROTECT	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.

	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
Rationale:	The OE.PERSON objective ensures competent administrators will manage the TOE, and the O.ADMIN objective ensures that there is a set of functions for administrators to use, and use is restricted to authorized users. The OE.INSTALL objective and the OE.PERSON objective ensure that administrators follow all provided documentation and maintain the security policy for installation and management of the TOE. The O.IDENTAUTH objective requires authentication of users prior to allowing access to TOE functions. The O.ACCESS objective builds upon the O.IDENTAUTH objective by permitting only authorized users to access TOE functions. The O.PROTECT objective addresses this policy by requiring TOE self-protection.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE. These users are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with TOE guidance documents.
	OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the system.
	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.INSTALL objective ensures that the TOE is properly installed and operated, and the OE.PHYSICAL objective provides for physical protection of the TOE. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.	

Assumption: **A.NETWORK**	The TOE components and their hosts are installed on an internal network which protects the data from disclosure and modification by untrusted systems or users.	
Objectives:	OE.NETWORK	The operational environment will provide a segregated, internal network that protects the traffic that passes between the TOE components from disclosure and modification by untrusted systems or users.
Rationale:	The OE.NETWORK objective ensures that the management traffic will be protected on an internal network.	

Assumption: **A.PROTECT**	The hardware and software critical to TOE security policy enforcement will be protected from unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	The OE.PHYSICAL objective provides for the physical protection of the TOE hardware and software components, and the hardware and software components that support the TOE implementation.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. The following extended SFR has been created to address additional security features of the TOE:

- User Data Backup/Restore (FDP_BCK_EXT.1)

5.1.1 Family FDP_BCK_EXT: User Data Backup/Restore

User Data Backup/Restore provides for the functionality to perform backup and restore operations as directed by administrators and users. The User Data Backup/Restore family was modeled after FDP_ACC: Access Control Policy. The User Data Backup/Restore SFR was loosely modeled after FDP_ACC.1: Subset access control.

Family Behaviour

This family defines the requirements for the TOE to provide backup and restore services for IT systems in the operational environment.

Component Levelling

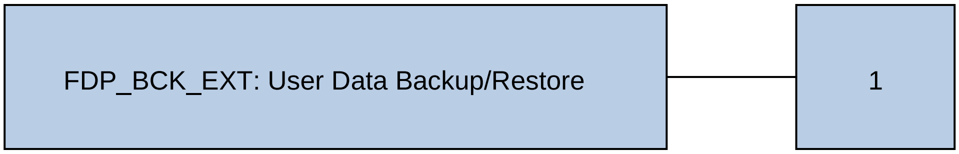

Figure 2 – FDP_BCK_EXT: User Data Backup/Restore Component Levelling

Management

The following actions could be considered for the management functions in FMT:

a) Configuration of the backup and restore operations to be performed.

Audit

There are no auditable events foreseen.

5.1.1.1 FDP_BCK_EXT.1 User Data Backup/Restore

Hierarchical to: No other components.

Dependencies: None

FDP_BCK_EXT.1.1 The TSF shall provide a capability to backup data and systems in accordance with the backup policy configured by authorized administrators.

FDP_BCK_EXT.1.2 The TSF shall provide a capability for authorized administrators to restore files to systems from previously-created backups.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2, are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Cryptographic Support (FCS)	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key Destruction
	FCS_COP.1	Cryptographic operation

Class	Identifier	Name
User Data Protection (FDP)	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_BCK_EXT.1	User Data Backup/Restore
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_STM.1	Reliable time stamps

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [not specified] level of audit; and

c) [*no other auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*no other audit relevant information*].

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation
	FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The TSF shall provide [*Master Server Root, NetBackup Administrator, Security Administrator, Backup Administrator*] with the capability to read [*all audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.3 Selectable audit review

Hierarchical to:	No other components.
Dependencies:	FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*filtering*] of audit data based on [*start time, end time, category, username*].

6.2.2 Cryptographic Support (FCS)

6.2.2.1 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*Counter Deterministic Random Bit Generator*] and specified cryptographic key sizes [*256 bits*] that meet the following: [*SP 800-90A*[3]].

6.2.2.2 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or
	FDP_ITC.2 Import of user data with security attributes, or
	FCS_CKM.1 Cryptographic key generation]

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-90A

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [*zeroization*] that meets the following: [*FIPS 140-2*].

6.2.2.3 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform [*data encryption and decryption*] in accordance with a specified cryptographic algorithm [*AES*[4]] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS 197*].

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] on [
Subjects: users
Objects: TSF data, backup data
Operations: configure backup, recover].

6.2.3.2 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] to objects based on the following: [
Subjects: users
Subject attributes: user role
Objects: TSF data, backup data
Object attributes: data source (system)].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [
users assigned a role with the appropriate privileges are able to modify TSF data to configure backup operations and initiate recovery operations].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

[4] Advanced Encryption Standard

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

6.2.3.3 FDP_BCK_EXT.1 User Data Backup/Restore

Hierarchical to: No other components.

Dependencies: None

FDP_BCK_EXT.1.1 The TSF shall provide a capability to backup data and systems in accordance with the backup policy configured by authorized administrators.

FDP_BCK_EXT.1.2 The TSF shall provide a capability for authorized administrators to restore files to systems from previously-created backups.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.4.2 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*obscured feedback*] to the user while the authentication is in progress.

6.2.4.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.5 Security Management (FMT)

6.2.5.1 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [query, modify, delete] the security attributes [*role*] to [*Master Server Root, NetBackup Administrator, Security Administrator*].

6.2.5.2 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies:	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Role Based Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [*Master Server Root, NetBackup Administrator, Security Administrator*] to specify alternative initial values to override the default values when an object or information is created.

6.2.5.3 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [*audit record review, encryption policy management, backup policy management, user management*].

6.2.5.4 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
Dependencies:	FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [*Master Server Root, NetBackup Administrator, Security Administrator, Backup Administrator*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_STM.1 Reliable time stamps

Hierarchical to:	No other components.
Dependencies:	No dependencies.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 11.

Assurance Class	Assurance Components	
	Identifier	Name
Development (ADV)	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents (AGD)	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-Cycle Support (ALC)	ALC_CMC.2	Use of a CM[5] system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation (ASE)	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests (ATE)	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing

[5] Configuration Management

Assurance Class	Assurance Components	
	Identifier	**Name**
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 11 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS	O.ADMIN	O.AUDIT	O.BACKUP	O.CRYPTO	O.IDENTAUTH	O.PROTECT	O.TIME
FAU_GEN.1			X					
FAU_GEN.2			X					
FAU_SAR.1			X					
FAU_SAR.3			X					
FCS_CKM.1					X			
FCS_CKM.4					X			
FCS_COP.1					X			
FDP_ACC.1				X			X	
FDP_ACF.1				X			X	
FDP_BCK_EXT.1				X				
FIA_UAU.2	X					X	X	
FIA_UAU.7	X					X		
FIA_UID.2	X					X	X	
FMT_MSA.1	X	X		X			X	
FMT_MSA.3		X		X			X	

	O.ACCESS	O.ADMIN	O.AUDIT	O.BACKUP	O.CRYPTO	O.IDENTAUTH	O.PROTECT	O.TIME
FMT_SMF.1		X					X	
FMT_SMR.1	X	X					X	
FPT_STM.1			X					X

Table 12 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS**	The TOE must allow authorized users to access only appropriate TOE functions and data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
	FMT_MSA.1	Management of security attributes
	FMT_SMR.1	Security roles
Rationale:	FIA_UID.2 and FIA_UAU.2 require users to be authenticated prior to gaining access to TOE functions. This ensures that only authorized users gain access to TOE functions and data. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE. FMT_MSA.1 defines which user roles have permissions to read and modify user roles for other users. FMT_SMR.1 ensures the TOE supports multiple roles so that appropriate data access can be provided to users with varied responsibilities.	

Objective: **O.ADMIN**	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE, and restrict these functions from unauthorized use.	
Security Functional	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation

Requirements:	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FMT_MSA.1 and FMT_MSA.3 define the access permissions, including default permissions, which determine the TSF data that is accessible to each role. FMT_SMF.1 specifies the management functionality required for effective management of the TOE. FMT_SMR.1 defines the roles required to provide effective management capabilities for users with different responsibilities.	

Objective: **O.AUDIT**	The TOE must generate audit records for security related events.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FPT_STM.1	Reliable time stamps
Rationale:	FAU_GEN.1 and FAU_GEN.2 require audit records to be generated for security related events and ensure that the user initiating the event is identified in the record. FAU_SAR.1 requires that audit records be available to authorized users for review. FAU_SAR.3 requires that the TOE provide functionality to filter the audit records for convenient viewing. FPT_STM.1 requires accurate time stamps to be available for the audit records.	

Objective: **O.BACKUP**	The TOE shall backup specified client data and make it available for restore operations.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_BCK_EXT.1	User data backup/restore
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation

Rationale:	FDP_ACC.1 and FDP_ACF.1 ensure that backup data is created as directed and is available to be restored as required. FDP_BCK_EXT.1 ensures that the TOE supports backup and restore operations. FMT_MSA.1 ensures that appropriate security attributes are maintained for subjects, and FMT_MSA.3 ensures that default role attributes are restrictive in nature.	

Objective: **O.CRYPTO**	Backup data must be protected using approved cryptographic functions.	
Security Functional Requirements:	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
Rationale:	FCS_CKM.1 and FCS_CKM.4 provide for key management in support of encryption of backup data. FCS_COP.1 provides the cryptographic operations required to encrypt backup data.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to TOE functions and data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Rationale:	FIA_UID.2 and FIA_UAU.2 ensure that administrative users are identified and authenticated, thus ensuring that only authorized persons have access to TSF data and backup data. FIA_UAU.7 protects the password from being observed, preventing unauthorized users from gaining access to the TOE.	

Objective: **O.PROTECT**	The TOE must ensure the integrity of all TSF data, including audit records, by protecting itself from unauthorized access.	
Security Functional Requirements:	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FIA_UAU.2	User authentication before any action

	FIA_UID.2	User identification before any action
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Rationale:	FDP_ACC.1 and FDP_ACF.1 define the access control policy that determines access to TSF data. FIA_UAU.2 and FIA_UID.2 ensure that users must be authenticated prior to access to TSF data, thereby preventing unauthorized access. FMT_MSA.1 and FMT_MSA.3 provide the functionality that determines the attributes used by the access control policy. FMT_SMR.1 provides the roles that are used to restrict access to TSF data.	

Objective: **O.TIME**	The TOE must provide reliable timestamps.	
Security Functional Requirements:	FPT_STM.1	Reliable time stamps
Rationale:	FPT_STM.1 requires the provision of accurate time stamps.	

6.4.3 Dependency Rationale

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	

SFR	Dependency	Dependency Satisfied	Rationale
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1	✓	Satisfied by FCS_COP.1
	FCS_CKM.4	✓	
FCS_CKM.4	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by FCS_CKM.1
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
FDP_BCK_EXT.1	None	✓	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_STM.1	None	N/A	

Table 13 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). EAL 2 was chosen for competitive reasons. The developer is claiming the ALC_FLR.2 augmentation since current practices and procedures exceed the minimum requirements for EAL 2.

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

7.1 SECURITY AUDIT

The NetBackup Audit Manager runs on the Master Server, where audit records are maintained in the database. Auditing is enabled by default.

The TOE is placed in enhanced auditing mode in the evaluated configuration. In the default configuration, only a root or a NetBackup Administrator can perform NetBackup operations through a command line interface or through the NetBackup Administration Console. The action is audited with ‘root’ or ‘administrator’ as the user name. When Enhanced Auditing is enabled, the name of the user who performed the NetBackup operation is included in the audit record. For actions performed using the Web UI, the username is always included, where appropriate.

Audit records contain the following information:

Field	Description
DESCRIPTION	The details of the action that was performed. The details include the new values that are given to a modified object and the new values of all attributes for a newly created object. The details also include the identification of any deleted objects.
USER	The identity of the user who performed the action. The identity includes the user name, the domain, and the domain type of the authenticated user.
TIMESTAMP	The time that the action was performed. The time is given in Coordinated Universal Time (UTC) and indicated in seconds.
CATEGORY	The category of user action that was performed.
ACTION	The action that was performed.
REASON	The reason that the action was performed. A reason displays if a reason was specified in the command that created the change.
DETAILS	An account of all of the changes, listing the old values and the new values. Displays only with the -fmt DETAIL|PARSABLE options.

Table 14 – Audit Record Contents

The following table details the audited events related to the NetBackup security claims.

Actions	Audited Events
Policy actions	Adding, deleting, or updating policy attributes, clients, schedules, and backup selections lists
Activity monitor actions	Canceling, suspending, resuming, restarting, or deleting any type of job creates an audit record
Storage units actions	Adding, deleting, or updating storage units
Storage servers actions	Adding, deleting, or updating storage servers
Disk pools and Volume pools actions	Adding, deleting, or updating disk or volume pools
Catalog information	Includes verifying and expiring images
User management	Adding and deleting users in the Enhanced Auditing mode
Host database	NetBackup host database related operations
Login attempts	Any successful or failed login attempts for NetBackup Administration Console
Security configuration	Information related to changes made to the security configuration settings
Starting a restore job	Starting a restore job
Starting and stopping the NetBackup Audit Manager (nbaudit)	Starting and stopping of the nbaudit manager is always audited, even if auditing is disabled.

Table 15 – Security-related Audit Events

The audit records are held in a database within the Master Server, and may be viewed through the CLI using the nbauditreport command. The following options are used to filter the audit records.

Option	Description
-sdate <"MM/DD/YY [HH:[MM[:SS]]]">	Used to indicate the start date and time of the report data to be viewed
-edate <"MM/DD/YY [HH:[MM[:SS]]]">	Used to indicate the end date and time of the report data to be viewed
-ctgy	Used to display records pertaining to a particular category. The security-related categories are: • POLICY • JOB • STU (storage units)

Option	Description
	• STORAGESRV • POOL • AUDITCFG • AUDSVC • LOGIN • AZFAILURE (authorization failure) • USER
-user <username[:domainname]>	Used to indicate the name of the user indicated in the audit information

Table 16 – Audit Record Filters

Audit records may also be viewed through the Web UI, and through 'Reports' on the NetBackup Administration Console; however, filtering options described here are not available through these interfaces.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.3.

7.2 CRYPTOGRAPHIC SUPPORT

NetBackup includes a Federal Information Processing Standard (FIPS)-validated cryptographic module named 'Veritas NetBackup Cryptographic Module, version 1.0' (Cryptographic Module Validation Program (CMVP) certificate # 2340). This module is used to provide the key management services and encryption of backup data. Encryption of backup data is performed using AES 256.

The vendor affirms that no source code changes were made to the cryptographic module prior to recompilation into the TOE software.

When performing a backup, the Media Server Deduplication (MSDP) plug-in on the client encrypts the data after the deduplication operation has been performed. The data remains encrypted during transfer to the NetBackup Media Server for storage. When backup data is restored, the encrypted data is transferred to the NetBackup client, where it is decrypted and restored.

This functionality is configured using the MSDP pd.conf file. The ENCRYPTION parameter determines how backup encryption is performed for individual hosts. By default, backup encryption is disabled. In the evaluated configuration, encryption is enabled on all TOE components.

TOE Security Functional Requirements addressed: FCS_CKM.1, FCS_CKM.4, FCS_COP.1.

7.3 USER DATA PROTECTION

7.3.1 Role Based Access Control

Role Based Access Control is used to govern access to the TSF data that determines how and when automated backups are run, and to the backup data that is used when data is restored.

Users are granted access to TSF and backup data through the TOE interfaces as follows:

The NetBackup Administration Console

The Master Server root user and NetBackup Administrators have full access to the NetBackup Administration Console.

Command Line Interface (CLI)

The Master Server root user and NetBackup Administrators have full access to the CLI.

Web User Interface (UI)

Users of the Web UI must be assigned the role of NetBackup Administrator, Security Administrator or Backup Administrator. The Master Server root also has full access to the Web UI.

TOE Security Functional Requirements addressed: FDP_ACC.1, FDP_ACF.1.

7.3.2 Backup and Recovery

NetBackup administrators can set up periodic or calendar-based schedules to perform automatic, unattended backups for clients across a network. The backups can be full or incremental: Full backups back up all indicated client files, while incremental backups back up only the files that have changed since the last backup.

During a backup, the client application sends backup data across the network to a NetBackup server. The NetBackup server manages the type of storage that is specified in the backup policy. During a restore, users can browse, and then select the files and directories to recover. NetBackup finds the selected files and directories and restores them to the disk on the client machine.

TOE Security Functional Requirements addressed: FDP_BCK_EXT.1.

7.4 IDENTIFICATION AND AUTHENTICATION

Identification and authentication services are provided by the underlying operating systems. Local users are created on the Red Hat and Windows systems in the evaluated configuration. Users must enter their credentials into the NetBackup interface, and NetBackup verifies that the users have been identified and authenticated prior to allowing them access to the NetBackup functions. Passwords are obscured as they are entered.

TOE Security Functional Requirements addressed: FIA_UAU.2, FIA_UAU.7, FIA_UID.2.

7.5 SECURITY MANAGEMENT

Security Management is performed using the following interfaces:

- **The NetBackup Administration Console** The NetBackup Administration Console is a java client that is installed on the Management Workstation and communicates with the Master Server over an internal, protected network. This interface may be used to review audit records, manage the encryption policy, manage the backup policy and manage users.
- **Command Line Interface (CLI)** The CLI is accessed directly on the Master Server. It may be used to review audit records, set encryption policy options, manage the backup policy and manage users.
- **Web User Interface (UI)** The Web UI may be used to review audit records, manage backup policy and manage users.

User administration, including the ability to query, modify and delete the user role, is limited to users in the Master Server root, NetBackup Administrator or Security Administrator roles. The default values are considered to be restrictive in that a user does not have a role until one is assigned. The administrator who creates the user is able to determine the user’s role at time of creation.

TOE Security Functional Requirements addressed: FMT_MSA.1, FMT_MSA.3, FMT_SMF.1.

7.5.1 Roles

The NetBackup Administrator and Master Server root user are able to perform all administrative functions using the NetBackup Administration Console, CLI and Web UI.

The Security Administrator is able to determine which users can access NetBackup, the role or permissions that these users have, and the NetBackup assets which these users can access. The Security Administrator is also able to manage global security settings, and view security events. Users in this role are able to perform administrative tasks through the Web UI only.

The Backup Administrator manages all jobs activity, and monitors all job operations. Users in this role are able to cancel, suspend, resume, restart, and delete jobs. Backup Administrators are able to view usage reporting details on backup data size for the NetBackup Master Server. Users in this role are able to perform administrative tasks through the Web UI only.

TOE Security Functional Requirements addressed: FMT_SMR.1.

7.6 PROTECTION OF THE TSF

Timestamps are provided by the operating system for use within NetBackup. This includes the provision of timestamps for audit records.

TOE Security Functional Requirements addressed: FPT_STM.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	This is a generic term used to refer to administrators in any role.
Administrator (windows)	The term Administrator (windows) is used to refer to the Administrator on a Microsoft Windows Server.
Client	The term ‘client’ refers to the people responsible for client machines subject to backup and recovery operations.
NetBackup Administrator	This is used to refer to a user assigned the Administrator role on the NetBackup system.
Users	The term ‘user’ refers to an administrative user of the NetBackup implementation.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
IT	Information Technology
MSDP	Media Server Deduplication
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PP	Protection Profile

Acronym	Definition
RHEL	Red Hat Enterprise Linux
SFP	Security Function Policy
SFR	Security Functional Requirement
SP	Special Publication
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
UTC	Coordinated Universal Time

Table 18 – Acronyms