Dell EMC™ NetWorker® 9.1

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 1986-000-D102
Version: 1.2
10 July 2017

EMC Corporation
176 South Street
Hopkinton, MA, USA
01748

Prepared by:
EWA-Canada
1223 Michael Street, Suite 200
Ottawa, Ontario, Canada
K1J7T2

Enabling a More Secure Future

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 ST reference, the TOE reference, the TOE overview and the TOE description.

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

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.

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:	Dell EMC™ NetWorker® 9.1 Security Target
ST Version:	1.2
ST Date:	10 July 2017

1.3 TOE REFERENCE

TOE Identification:	Dell EMC™ NetWorker® 9.1.0.5 build 89
TOE Developer:	EMC Corporation
TOE Type:	Backup and Recovery Solution (Data Protection)

1.4 TOE OVERVIEW

EMC NetWorker is a backup and recovery solution that provides robust access control, authentication and auditing. It is implemented as a collection of services on Windows and Linux based systems, as well as several Command Line Interfaces (CLIs) and Graphical User Interfaces (GUIs). An administrator may initiate NetWorker functions either from within the GUI-based NetWorker Management Console (NMC) Applet or from a set of NetWorker command-line interfaces. Additionally, end users of client systems can perform ad-hoc backup and restore operations.

The evaluated configuration of the TOE consists of four major components:

- NetWorker Server and Authentication Service software running on a dedicated Linux instance on general purpose computing hardware
- NetWorker Client software running in two separate instances on general purpose computing hardware for:
  - Windows Server 2008 R2
  - Linux (Red Hat Enterprise Linux 6.6)
- NetWorker Storage Node software running on a dedicated Linux instance on general purpose computing hardware with an attached storage device
- NMC Server software running on a dedicated Linux instance on general purpose computing hardware. The NMC Server delivers the NMC Applet, which runs from a Java Virtual Machine within a supported web browser

The TOE is a software only TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

Figure 1 shows the deployment for the evaluated configuration. Note that the lines indicate the primary communications paths only. Figure 2 shows the TOE Boundary.

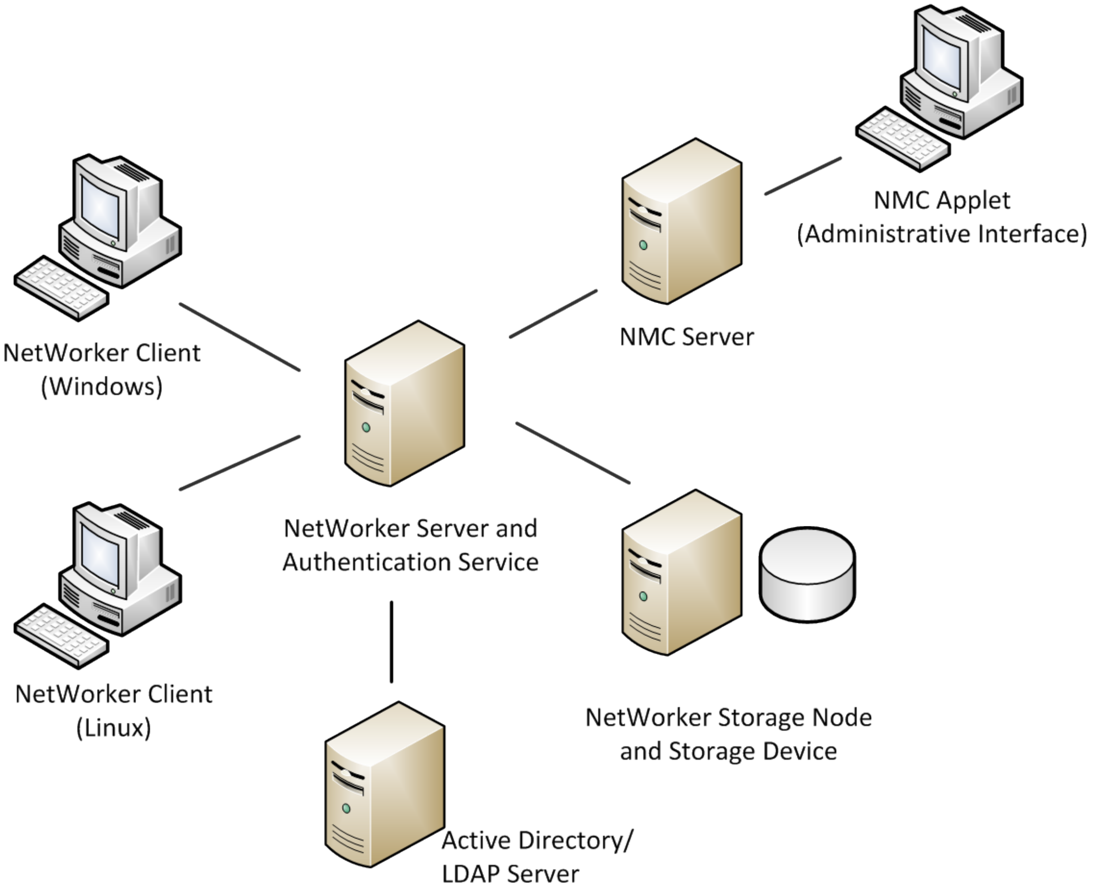

Figure 1 – TOE Diagram

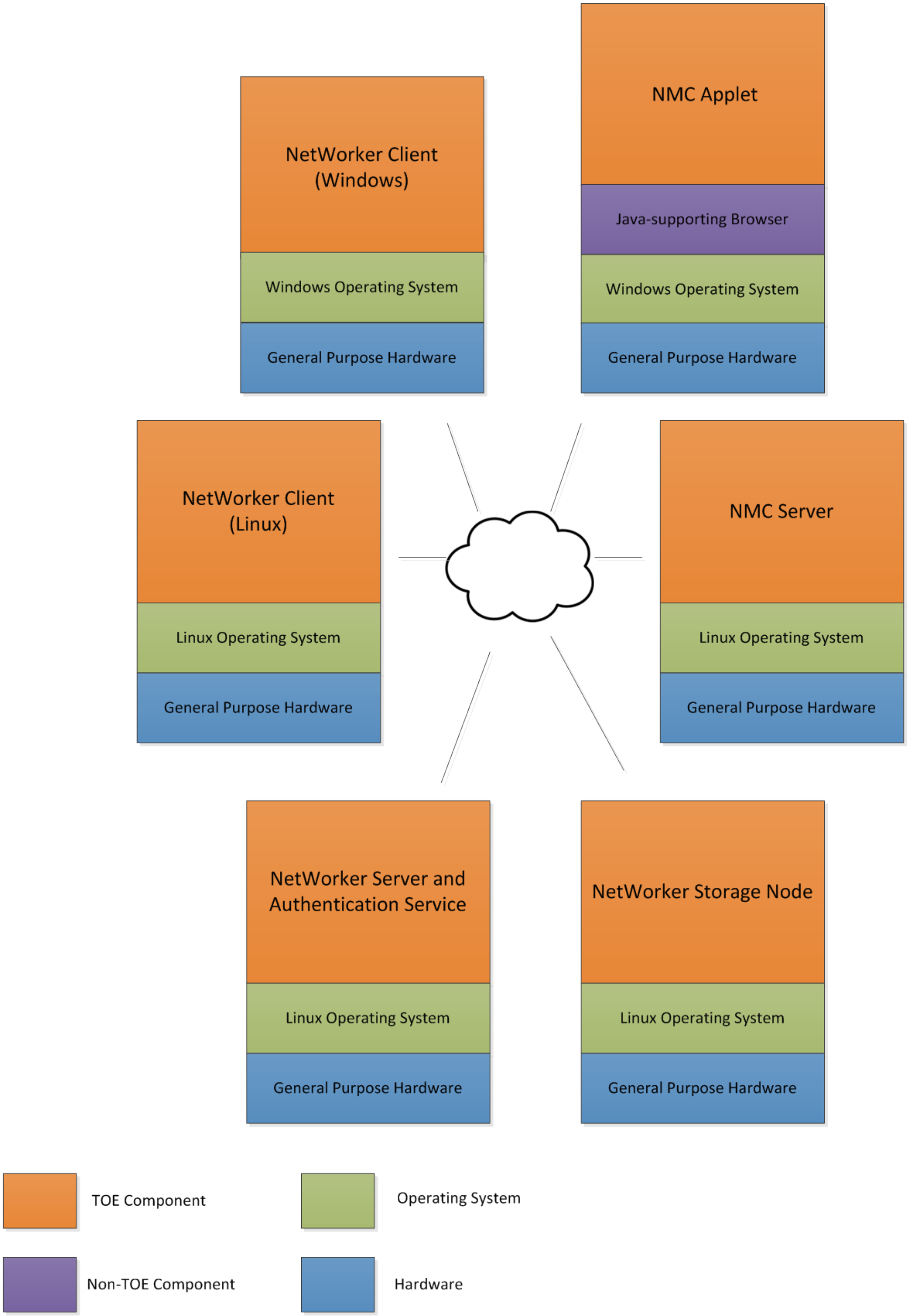

Figure 2 – TOE Boundary

The evaluated configuration of EMC NetWorker is made up of the following components:

- NetWorker Server (with the Auth-C authentication service)
- NetWorker Client (on both Red Hat Enterprise Linux 6.6 and Windows Server 2008 R2)
- NetWorker Storage Node
- NetWorker Management Console (NMC) Server, including the downloadable NMC Applet

Additionally, a customer would be required to implement the EMC Electronic License Management Server (ELMS). This is required to install and configure NetWorker, but is not involved in the day to day operation of the software, or the enforcement of the security claims.

1.5.1.1 NetWorker Server

Each NetWorker Server provides backup/recovery scheduling, queuing and coordination, and management of data lifecycles, volume pools, client indexes, and media databases.

The Server coordinates backup operations. This involves defining the save sets to be backed up, creating entries for the client index and media database structures, and coordinating volume pools for receiving backup data. Write operations require server coordination to optimize performance by taking advantage of server parallelism and managing writes between local and remote storage nodes. Recover operations require the server to manage reads from the volumes and to optimize performance through server parallelism. Server parallelism controls how many total streams from all its clients a NetWorker Server allows to be simultaneously active for the purposes of backup or recovery. Data lifecycle operations require that the server routinely compare the age and status of stored data with policies specified by the administrator, and take the action required to implement those policies. Volume management operations require the server:

a. to locate volumes required by operations, and to automatically mount, unmount, and label those volumes as needed;

b. to inventory autochangers; and

c. to clone and stage data from one volume to another as requested.

The NetWorker Server includes the Authentication Service. This service provides users with an authentication token that is supplied with each subsequent request.

1.5.1.2 NetWorker Client

The NetWorker client software provides client-initiated backup and recovery functionality and communicates with the other NetWorker components. The NetWorker Client software is installed on all computers that are backed up in the NetWorker implementation.

1.5.1.3 NetWorker Storage Node

The NetWorker Storage Node software is installed on a computer resource with directly connected storage devices. The Storage Node software is installed by default with the NetWorker Server, but is installed on a separate machine in the evaluated configuration.

Data may be backed up directly to storage resources associated with the NetWorker Server or may be sent to a NetWorker Storage Node. A storage node controls storage devices such as tape drives, disk devices, autochangers, and silos. Using a storage node off-loads much of the data transfer involved in backup and recovery operations from the NetWorker Server, thereby improving overall performance.

1.5.1.4 NetWorker Management Console Server

The NetWorker Management Console (NMC) Server is a Java-based web application server that provides centralized management, monitoring, and reporting of backup operations for NetWorker Servers and NetWorker Clients across multiple datazones. The NMC Server is accessed through a GUI that may be run from any computer with a supported web browser and Java Runtime Environment (JRE).

1.5.2 TOE Environment

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

TOE Component	Supporting Software and Operating System	Supporting Hardware
NetWorker Server	Red Hat Enterprise Linux 6.6	General Purpose Computing Hardware
Authentication Service	Red Hat Enterprise Linux 6.6	General Purpose Computing Hardware
NMC	Red Hat Enterprise Linux 6.6	General Purpose Computing Hardware
NMC Applet	Browser (Mozilla FireFox 52) Windows 7 SP1	General Purpose Computing Hardware
NetWorker Storage Node	Red Hat Enterprise Linux 6.6	General Purpose Computing Hardware
Windows Client	Windows Server 2008 R2	General Purpose Computing Hardware

TOE Component	Supporting Software and Operating System	Supporting Hardware
Linux Client	Red Hat Enterprise Linux 6.6	General Purpose Computing Hardware

Table 1 – TOE Components and Non-TOE Hardware and Software

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- EMC® NetWorker® Version 9.1 Installation Guide
- EMC® NetWorker® Version 9.1 Administration Guide
- EMC® NetWorker® Version 9.1 Command Reference Guide
- EMC® NetWorker® Version 9.1 Security Configuration Guide
- EMC® NetWorker® Version 9.1 Error Message Guide

1.5.4 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 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs are stored and protected from unauthorized modification and deletion.
User Data Protection	The TOE provides a role-based access control capability to ensure that only authorized administrators are able to administer the TOE. The TOE provides backup and recovery functionality.
Identification and Authentication	Users must identify and authenticate prior to gaining TOE access.
Security Management	The TOE provides management capabilities via a Web-Based GUI and through a CLI. Management functions allow the administrators to perform system configuration, user management, and backup and recovery operations.
Protection of the TSF	A retention setting may be applied to save sets indicating the date before which the save set may not be deleted.
TOE Access	A banner is presented on user login to the NMC.

Table 2 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Although NetWorker supports backup and recovery from many different platforms, only Windows and Linux were evaluated.
- Integration with other EMC products was not evaluated.

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-2012-09-001, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2012-09-002, Version 3.1, Revision 4, September 2012
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components CCMB-2012-09-003, Version 3.1, Revision 4, September 2012

As follows:

- CC Part 2 conformant
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012 has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

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

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Table 3 lists the threats addressed by the TOE. Potential threat agents are authorized TOE users, and unauthorized persons. The level of expertise of both types of attacker is assumed to be unsophisticated. TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations, and to possess a high level of skill. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile. Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters and no physical access to the TOE.

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

Threat	Description
T.DATALOSS	A user or system failure may cause the loss of critical user data resulting in users being unable to continue their work.
T.UNAUTH	An unauthorized user may be able to view recovery files or access security management functions, resulting in unauthorized access to user data.
T.UNDETECT	Authorized or unauthorized users may be able to access TSF or user data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

There are no Organizational Security Policies applicable to this TOE.

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE.
A.NOEVIL	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Assumptions	Description
A.TIME	The operational environment provides the TOE with reliable timestamps.

Table 4 – 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, 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.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must advise users of possible unauthorized use, and restrict security management functions from unauthorized use.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and must protect the stored audit records to prevent unauthorized modification or removal.
O.BACKUP	The TOE must implement backup and recovery functionality that restricts access to backed-up data to owners and authorized administrators.
O.IDENTAUTH	The TOE must be able to ensure that users are identified and authenticated prior to gaining access to the administrative functions, TSF data or user data.

Table 5 – 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.MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
OE.PROTECT	Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack.
OE.TIME	The operational environment must provide reliable timestamps for use by the TOE.

Table 6 – 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.DATALOSS	T.UNAUTH	T.UNDETECT	A.LOCATE	A.MANAGE	A.NOEVIL	A.TIME
O.ADMIN		X					
O.AUDIT			X				
O.BACKUP	X						
O.IDENTAUTH		X					
OE.MANAGE					X	X	
OE.PROTECT				X			
OE.TIME							X

Table 7 – 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 back to the threats addressed by the TOE.

Threat:	A user or system failure may cause the loss of critical user data

T.DATALOSS	resulting in users being unable to continue their work.	
Objectives:	O.BACKUP	The TOE must implement backup and recovery functionality that restricts access to backed-up data to owners and authorized administrators.
Rationale:	O.BACKUP mitigates the threat by ensuring that the TOE provides backup and recovery functionality that affords access to critical user data even if the original data is lost.	

Threat: **T.UNAUTH**	An unauthorized user may be able to view recovery files or access security management functions, resulting in unauthorized access to user data.	
Objectives:	O.ADMIN	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must advise users of possible unauthorized use, and restrict security management functions from unauthorized use.
	O.IDENTAUTH	The TOE must be able to ensure that users are identified and authenticated prior to gaining access to the administrative functions, TSF data or user data.
Rationale:	O.ADMIN mitigates this threat by ensuring that only authorized administrators may access security management functions of the TOE. O.IDENTAUTH mitigates this threat by ensuring that administrators and users are identified and authenticated prior to being granted access to security management functions or user data.	

Threat: **T.UNDETECT**	Authorized or unauthorized users may be able to access TSF or user data or modify TOE behaviour without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and must protect the stored audit records to prevent unauthorized modification or removal.
Rationale:	O.AUDIT mitigates this threat by ensuring audit records are created to make note of access to TSF and user data.	

4.3.2 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.LOCATE**	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PROTECT	Those responsible for the TOE must ensure that TOE components are protected from interference, tampering and physical attack.
Rationale:	OE.PROTECT supports this assumption by protecting TOE components from physical attack.	

Assumption: **A.MANAGE**	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
Rationale:	OE.MANAGE supports this assumption by ensuring that competent, trained individuals who follow guidance are in place to manage the TOE.	

Assumption: **A.NOEVIL**	The authorized administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.	
Objectives:	OE.MANAGE	Those responsible for TOE deployment will provide competent administrators who are appropriately trained and follow all guidance.
Rationale:	OE.MANAGE supports this assumption by ensuring that the individuals managing the TOE are competent, trained and follow all guidance.	

Assumption: **A.TIME**	The operational environment provides the TOE with reliable timestamps.	
Objectives:	OE.TIME	The operational environment must provide reliable timestamps for use by the TOE.

Rationale:	OE.TIME supports this assumption by ensuring that the operational environment provides reliable timestamps.

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

This ST does not include extended Security Functional Requirements.

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, 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 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC, and are summarized in Table 9 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_STG.1	Protected audit trail storage
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control (RBAC)
	FDP_ACC.1(2)	Subset access control (Backup and Recovery)
	FDP_ACF.1(1)	Security attribute based access control (RBAC)
	FDP_ACF.1(2)	Security attribute based access control (Backup and Recovery)
Identification and	FIA_UAU.2	User authentication before any action

Class	Identifier	Name
Authentication (FIA)	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_MSA.1(1)	Management of security attributes (RBAC)
	FMT_MSA.1(2)	Management of security attributes (Backup and Recovery)
	FMT_MSA.3(1)	Static attribute initialisation (RBAC)
	FMT_MSA.3(2)	Static attribute initialisation (Backup and Recovery)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners

Table 8 – 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) [*configuration changes*, *backup and recovery 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 information*].

6.2.1.2 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [prevent] unauthorised modifications to the stored audit records in the audit trail.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1(1) Subset access control (RBAC)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*RBAC SFP*] on [
Subjects: NMC Administrators, NetWorker Server Administrators
Objects: TSF data, User data
Operations: Management operations
].

6.2.2.2 FDP_ACC.1(2) Subset access control (Backup and Recovery)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*Backup and Recovery SFP*] on [
Subjects: Users, Administrators
Objects: User Data, Save sets
Operations: Backup, Recovery
].

6.2.2.3 FDP_ACF.1(1) Security attribute based access control (Role-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(1) The TSF shall enforce the [*RBAC SFP*] to objects based on the following: [
Subjects: NMC Administrators, NetWorker Server Administrators[1]
Subject Attributes: Role
Objects: TSF data, User data
Object Attributes: none
].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*an administrator may access TSF data and User data to perform*

[1] NMC Server Administrators are administrative users that use the NMC component. NetWorker Server Administrators are administrative users that use the NetWorker Server component.

management functions if the administrator's role permits access to that function].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no other rules*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.2.4 FDP_ACF.1(2) Security attribute based access control (Backup and Recovery)

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

FDP_ACF.1.1(2) The TSF shall enforce the [*Backup and Recovery SFP*] to objects based on the following: [
Subjects: Users, Administrators
Subject Attributes: User identity for Users, Role for Administrators
Objects: User data, Save sets
Object Attributes: Save set identifier].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*identified users may backup their own data and recover their own save sets*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no other rules*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no other rules*].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 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.

6.2.3.2 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.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MSA.1(1) Management of security attributes (RBAC)

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(1) The TSF shall enforce the [RBAC SFP] to restrict the ability to [query, modify, delete] the security attributes [*TSF data*] to [*NMC Administrators, NetWorker Server Administrators*].

6.2.4.2 FMT_MSA.1(2) Management of security attributes (Backup and Recovery)

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(2) The TSF shall enforce the [Backup and Recovery SFP] to restrict the ability to [query, [*create*, *recover*]] the security attributes [*save sets, save set identifiers*] to [*Administrators with backup and recover permissions*].

6.2.4.3 FMT_MSA.3(1) Static attribute initialisation (RBAC)

Hierarchical to: No other components.

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

FMT_MSA.3.1(1) The TSF shall enforce the [*RBAC SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(1) The TSF shall allow the [*users in roles with the appropriate privileges*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_MSA.3(2) Static attribute initialisation (Backup and Recovery)

Hierarchical to: No other components.

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

FMT_MSA.3.1(2) The TSF shall enforce the [*Backup and Recovery SFP*] to provide [permissive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2(2) The TSF shall allow the [*users in roles with the appropriate privileges*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.5 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: [*system configuration, user management, backup and recovery*].

6.2.4.6 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 [*NMC Console Security Administrator, NMC Console Application Administrator, NMC Console User, Security Administrator, Application Administrator, Auditor, NetWorker Server User*].

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

Application Note: NetWorker Server supports additional default roles; however, only those noted in FMT_SMR.1.1 are demonstrated in the evaluated configuration.

6.2.5 TOE Access (FTA)

6.2.5.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a**n** [***administrator-configurable period of time***].

Application Note: The assignment in this SFR has been refined to show that a session is terminated after a configured period of time, rather than inactivity.

6.2.5.2 FTA_TAB.1 Default TOE access banners

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAB.1.1 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

Application Note: This SFR applied to the NMC Server login window when logging into the NMC Console. It does not apply to the command line interfaces.

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

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

	O.ADMIN	O.AUDIT	O.BACKUP	O.IDENAUTH
FAU_GEN.1		X		

	O.ADMIN	O.AUDIT	O.BACKUP	O.IDENAUTH
FAU_STG.1		X		
FDP_ACC.1(1)	X			
FDP_ACC.1(2)			X	
FDP_ACF.1(1)	X			
FDP_ACF.1(2)			X	
FIA_UAU.2				X
FIA_UID.2				X
FMT_MSA.1(1)	X			
FMT_MSA.1(2)	X			
FMT_MSA.3(1)	X			
FMT_MSA.3(2)	X			
FMT_SMF.1	X			
FMT_SMR.1	X			
FTA_SSL.3	X			
FTA_TAB.1	X			

Table 9 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

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

Objective: **O.ADMIN**	The TOE will provide all the functions necessary to support the administrators in their management of the security of the TOE. The TOE must advise users of possible unauthorized use, and restrict security management functions from unauthorized use.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control (RBAC)
	FDP_ACF.1(1)	Security attribute based access control (RBAC)
	FMT_MSA.1(1)	Management of security attributes (RBAC)
	FMT_MSA.1(2)	Management of security attributes (Backup

		and Recovery)
	FMT_MSA.3(1)	Static attribute initialisation (RBAC)
	FMT_MSA.3(2)	Static attribute initialisation (Backup and Recovery)
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination
	FTA_TAB.1	Default TOE access banners
Rationale:	FDP_ACC.1(1) and FDP_ACF.1(1) ensure that access to administrative functions is restricted to authorized administrators with the required privileges. FMT_MSA.1(1) ensures that access to the TSF data supporting security management functions is restricted to authorized NMC and NetWorker Server Administrators. FMT_MSA.3(1) ensures that default values for the security attributes that make up that TSF data are restrictive. FMT_MSA.1(s) ensures that access to save set data is restricted to authorized Administrators. FMT_MSA.3(1) ensures that default values for the security attributes associated with save sets are permissive. FMT_SMF.1 provides security management functionality to support system configuration, user management and backup and recovery operations. FMT_SMR.1 provides the security roles for users of the NMC and NetWorker Server. FTA_SSL.3 protects the security management functions from unauthorized use by ensuring that the session token times out after an administrator-configurable period of time. FTA_TAB.1 advises users of possible unauthorized use.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions, and must protect the stored audit records to prevent unauthorized modification or removal.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_STG.1	Protected audit trail storage
Rationale:	FAU_GEN.1 ensures that use of TOE functions is recorded, and defines the information that must be included in audit records. FAU_STG.1 ensures that the audit records are protected from unauthorized modification or removal.	

Objective: **O.BACKUP**	The TOE must implement backup and recovery functionality that restricts access to backed-up data to owners and authorized administrators.	
Security Functional Requirements:	FDP_ACC.1(2)	Subset access control (Backup and Recovery)
	FDP_ACF.1(2)	Security attribute based access control (Backup and Recovery)
Rationale:	FDP_ACC.1(2) and FDP_ACF.1(2) ensure that access to save sets is restricted to owners and authorized administrators.	

Objective: **O.IDENTAUTH**	The TOE must be able to ensure that users are identified and authenticated prior to gaining access to the administrative functions, TSF data or user data.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_UID.2 ensures that users are identified prior to being granted access to security management and backup and recovery operations. FIA_UAU.2 ensures that users are authenticated prior to being granted access to security management and backup and recovery operations.	

6.4 DEPENDENCY RATIONALE

Table 11 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	✓	The dependency is satisfied in the operational environment by OE.TIME.
FAU_STG.1	FAU_GEN.1	✓	
FDP_ACC.1 (1)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(1).
FDP_ACF.1 (1)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(1).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(1).

SFR	Dependency	Dependency Satisfied	Rationale
FDP_ACC.1 (2)	FDP_ACF.1	✓	Satisfied by FDP_ACF.1(2).
FDP_ACF.1 (2)	FDP_ACC.1	✓	Satisfied by FDP_ACC.1(2).
	FMT_MSA.3	✓	Satisfied by FMT_MSA.3(2).
FIA_UAU.2	FIA_UID.1	✓	Satisfied by FIA_UID.2, which is hierarchical to FIA_UID.1.
FIA_UID.2	None	N/A	
FMT_MSA.1(1)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(1).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1(2)	FDP_ACC.1 or FDP_IFC.1	✓	Satisfied by FDP_ACC.1(2).
	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3(1)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(1).
	FMT_SMR.1	✓	
FMT_MSA.3(2)	FMT_MSA.1	✓	Satisfied by FMT_MSA.1(2).
	FMT_SMR.1	✓	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	
FTA_SSL.3	None	N/A	
FTA_TAB.1	None	N/A	

Table 10 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

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 there are areas where current practices and procedures exceed the minimum requirements for EAL 2.

The assurance requirements are summarized in Table 12.

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 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
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 11 – Security Assurance Requirements

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 TOE SECURITY FUNCTIONS

A description of each of the TOE security functions follows.

7.1.1 Security Audit

The logging service runs on the NetWorker Server, and records security relevant events from both the NetWorker Server and from the clients defined to be in the NetWorker Server’s datazone. Security relevant events include configuration changes, user and group changes and backup and recovery events. The NMC component also logs events, including console activities. In the evaluated configuration, NetWorker user auditing must be enabled.

The audit records are stored on the NetWorker Server and the NMC Server. The logs may only be removed by those with delete permissions on the underlying operating system. NetWorker provides no means to modify the logs.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_STG.1.

7.1.2 User Data Protection

7.1.2.1 Role Based Access Control

NetWorker implements role-based access control to mediate the actions that may be performed by administrators. (It should be noted that the CC term ‘Role’ refers to the functionality called 'User authorization' in the NetWorker Security Configuration Guide.) User authorization settings control the rights or permissions that are granted to a user and enable access to a resource managed by NetWorker.

7.1.2.1.1 NMC

When an NMC user connects to the NMC server and enters a valid username and password, the http daemon on the NMC server downloads the Java client to the NMC client. The NMC server contacts the NetWorker Authentication Service to validate the user log in credentials. When the NetWorker Authentication Service successfully validates the credentials, the application issues an authentication token for the user, to the NMC Server. The NMC Server caches the token. When the user tries to establish a connection to the NetWorker Server by opening the NetWorker Administration window, the NMC server confirms that the user has access permissions to manage the NetWorker Server. If the user has the appropriate permissions, the NMC server sends the token to the NetWorker Server. The privileges assigned to an authenticated user on the NetWorker Server are based on the entries present in the Users or External roles attribute of the User Group resources on the NetWorker Server. User group membership defines which NetWorker activities the user is authorized to perform.

The user role used to connect to the NMC Server determines the level of access to the NMC Server functionality. The NMC Server restricts user privileges using three authorization roles. These roles cannot be deleted, and the privileges associated with these roles cannot be changed.

The NMC Console Security Administrator may:

- Add, delete, and modify NetWorker Authentication Service local database users
- Control user access to managed applications, such as a NetWorker server

The NMC Console Application Administrator may:

- Configure NMC system options
- Set retention policies for reports
- View custom reports
- Specify the NetWorker Server to back up the NMC database
- Specify a NetWorker License Manager server
- Run the Console Configuration wizard
- Perform all tasks available to a Console User role

The NMS Console User may perform all tasks except for those tasks that are explicitly mentioned for the NMC Console Security Administrator and the NMC Console Application Administrator. Tasks include:

- Add and delete hosts and folders
- Add and delete Managed applications for NetWorker
- Create and delete the user’s own reports
- Set features for Managed Applications
- Manage a NetWorker Server with the appropriate privilege levels
- Dismiss events

7.1.2.1.2 NetWorker Server

Token-based authentication is also used with the command line when accessing the NetWorker Server. The user first runs the ‘nsrlogin’ command. The host machine contacts the NetWorker Authentication Service to validate the user log in credentials. (Note that in the evaluated configuration, the Authentication Service is located with the NetWorker Server.) When the NetWorker Authentication Service successfully validates the credentials, the application issues an authentication token to the host for the user account that was used to run the command. The host caches the token and confirms that the user account has the appropriate privileges to perform the operation for the commands that are then issued. The administrator may perform CLI commands until the token expires, at which time, the administrator must re-authenticate to continue.

The NetWorker Server roles are provided using preconfigured user groups with specific privileges. The preconfigured user groups may not be deleted, but privileges may be altered for all but the Security Administrators and Application Administrators groups. There are additional preconfigured roles not being claimed for this evaluation.

The following table provides a summary of the claimed preconfigured user groups and the default privileges associated with each user group.

Role (User Group)	Privileges
Security Administrators	View Security Settings
	Change Security Settings
	Create Security Settings
	Delete Security Settings
Application Administrators	Remote Access All Clients
	Configure NetWorker
	Backup Local Data
	Backup Remote Data
	Operate NetWorker
	Monitor NetWorker
	Operate Devices and Jukeboxes
	Recover Local Data
	Recover Remote Data
	Create Application Settings
	View Application Settings
	Change Application Settings
	Delete Application Settings
	Archive Data
Auditors	View Security Settings
Users	Monitor NetWorker
	Recover Local Data
	Backup Local Data

Table 12 – NetWorker Server Roles and Privileges

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

7.1.2.2 Backup and Recovery

Access to backup and recovery functionality is based on user identity. A user may backup and recover his or her own data.

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.1.3 Identification and Authentication

Identification and authentication functionality is provided by the NetWorker Authentication Service, which is installed on the NetWorker Server.

A token-based authentication is used to enable users to securely connect to the NMC Server, the NetWorker Server, and to perform secure backup and recovery operations. When a NetWorker or NMC operation requires authentication, the requesting process contacts the NetWorker Authentication Service to verify the credentials of the user account that started the request. When the NetWorker Authentication Service successfully identifies and authenticates the user, the application issues a time-limited, signed, and encrypted Security Assertion Markup Language (SAML) token to the requesting process. All the NetWorker components that require authentication can use the token to verify the user, until the token expires.

In the evaluated configuration, the NetWorker Authentication Service may authenticate users locally, or contact a Lightweight Directory Access Protocol (LDAP) Directory such as Active Directory (AD) to perform that function. CLI users are expected to use the ‘nsrlogout’ command to end the authenticated session.

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

7.1.4 Security Management

NMC Administrators and NetWorker Server Administrators may query, modify and delete user and TSF data in order to perform management functions permitted in accordance with the administrative role assigned to that user.

The default values for the security attribute ‘Role’ used in the RBAC SFP is considered to be restrictive. The user has no administrative role until specifically assigned by an administrator with the appropriate privilege. Roles may be changed by administrative users in roles with the appropriate combination of the following permissions:

- Create Security Settings
- View Security Settings
- Change Security Settings
- Delete Security Settings

The Backup and Recovery SFP allows non-administrative users to backup and recover their own data. It also allows NMC and NetWorker Server Administrators in a role with the ‘Backup Local Data’ and ‘Recover Local Data’ or ‘Backup

Remote Data' and 'Recover Remote Data' permissions the ability to perform these tasks.

The default values for the security attributes save set and save set identifier are considered permissive. By default, all users are permitted to backup and recover their own data. This may be restricted by an administrator in a role with the 'Operate NetWorker' permission.

The primary interfaces for accessing security management functionality are the NMC Administrative GUI and the NetWorker Server CLI. These interfaces support system configuration, user management and backup and recovery functionality.

The NMC Server supports three roles: NMC Console Security Administrator, NMC Console Application Administrator and NMC Console User. These roles cannot be deleted and the permissions associated with these roles may not be changed. Four of the default NetWorker Server roles are included in the evaluated configuration. They are Security Administrator, Application Administrator, Auditor and NetWorker Server User. New NetWorker Server roles may be created. With the exception of the Application Administrators and the Security Administrator roles, roles may be modified by changing the associated privileges.

TOE Security Functional Requirements addressed: FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3(1), FMT_MSA.3(2), FMT_SMF.1, FMT_SMR.1.

7.1.5 TOE Access

In order to perform TSF-mediated actions, users must obtain a token either by logging into the NMC Administrative GUI, or running the nsrlogin command from the command line. The authentication token is valid for an administrator-configurable period of time. This validity period is defined in the NetWorker Authentication Service. The default value is eight hours, and may be changed using the 'authc_config' command. When operated in the evaluated configurations, administrators are expected to run the nsrlogout command to closeout the interactive session.

A log-on banner is displayed in the NMC server login window. This message may be configured by an NMC Administrator by going to **Setup > System Options > Log-on banner**.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_TAB.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology is used in this ST:

Term	Description
Administrator	The term 'Administrator' is used to describe any user in a role with NMC or NetWorker Server administrative permissions. This includes users in the NetWorker Server User role.
NetWorker Server Administrator	NetWorker Server Administrators are administrators that use the NetWorker Server component interfaces. This includes users in the Security Administrator, Application Administrator, Auditor and NetWorker Server User roles.
NMC Administrator	NMC Administrators are administrators that use the NMC component. This includes users in the NMC Console Administrator, NMC Console Application Administrator and NMC Console User roles.
Save set	The collection of data items that are backed up during a backup session between the NetWorker server and a Client resource is called a save set. A save set can consist of the following: • A group of files or entire file systems • Application data, such as a database, or operating system settings
User	The term 'User' refers to any user of the NetWorker backup and recovery functionality. This role does not require access to NetWorker Server functionality, and should not be confused with the NetWorker Server User role.

Table 13 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AD	Active Directory
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CLI	Command Line Interface

Acronym	Definition
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ELMS	EMC Electronic License Management Server
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
NMC	NetWorker Management Console
OSP	Organizational Security Policy
PP	Protection Profile
RBAC	Role Based Access Control
RSA	Rivest, Shamir and Adleman
SAML	Security Assertion Markup Language
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

Table 14 – Acronyms