EMC Corporation
EMC® NetWorker® v8.0.1.4

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.1

Prepared for:

EMC²
where information lives®

EMC Corporation
176 South Street
Hopkinton, MA 01748
United States of America

Phone: +1 508 435 1000
http://www.emc.com

Prepared by:

Corsec®

Corsec Security, Inc.
13135 Lee Jackson Memorial Hwy., Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
http://www.corsec.com

Table of Contents

Table of Figures

List of Tables

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is EMC NetWorker® v8.0.1.4, and will hereafter be referred to as the TOE throughout this document. The TOE is a software-based, distributed, multi-platform tape and disk backup and recovery solution that provides advanced data integrity and confidentiality protection mechanisms.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements and objectives.
- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms and Terms (Section 9) – Defines the acronyms and terminology used within this ST.

1.2 Security Target and TOE References

Table 1 below depicts the ST and TOE references.

Table 1 ST and TOE References

ST Title	EMC Corporation EMC® NetWorker® v8.0.1.4 Security Target
ST Version	Version 1.1
ST Author	Corsec Security, Inc.
ST Publication Date	10/29/2013
TOE Reference	EMC® NetWorker® v8.0.1.4 build 163
FIPS[1] 140-2 Status	Level 1, RSA® BSAFE® Crypto-C Micro Edition 3.0.0.1, Certificate No. 1092

[1] FIPS – Federal Information Processing Standard

1.3 Product Overview

EMC NetWorker is a network-based backup software solution that centralizes, automates, and accelerates data backup and recovery across the IT[2] environment. NetWorker provides data protection for a wide variety of operating systems and data types. NetWorker reproduces online file system data at a protected location, while it maintains location and obsolescence tracking information about the data. NetWorker can then re-create the data if the online version is inadvertently changed, lost, or corrupted. NetWorker features include a storage management application that directs high performance writes to a range of storage devices, either local or remote.

The core functionality of NetWorker involves user data backup and recovery. NetWorker supports scheduled backup operations in addition to manual backups. Backups may also be performed on backup groups, representing a group of NetWorker clients that need to be backed up at the same time. Save sets, which identify the client resources to be backed up, may be used to backup individual files and directories, entire file systems, as well as several third party database applications. Browse and retention policies provide timely access to recent backups as well as protection of save set data from overwrites.

In addition to standard scheduled or manual backups, NetWorker supports various other types of backups. These include:

- **Synthetic full backups** – Synthetic full backups combine a full backup and subsequent incremental backups to form a new full backup.
- **Probe-based backups** – Probe-based backups are based on user-defined events for clients and NetWorker modules, in addition to time-based events.
- **Client direct backups –** Using client direct backups, clients with access to Advanced File Type Devices and Data Domain Boost storage devices to send their backup data directly to the devices, bypassing the NetWorker storage node.
- **CheckPoint restart backups –** CheckPoint restart backups allow for a failed backup operation to restart at a known good point, prior to the point-of-failure during the backup.
- **Deduplication backups –** NetWorker provides integration with EMC Avamar and EMC Data Domain for deduplication of backup data.
- **NDMP[3] support –** The NetWorker server facilitates the backup of NDMP-enabled NAS[4] appliances. The NetWorker server acts as a Data Management Application, receiving file index data for direct-to-tape backups (Local/Direct Backup), or it can also be used to direct NDMP backup data to another NAS device (Three-Way) or a device attached to a NetWorker storage node.
- **Archiving –** Archiving involves capturing files and directories as they exist at a specific time, and writes the data to archive storage volumes, which are not recycled as part of a backup scheme, thus, they have no expiration date.
- **Cloning –** Save sets and volumes can be "cloned", which involves transferring the data from one location to another and verifying the backups.

NetWorker also provides the capability to roll back NetWorker client-protected computers to a previous state using two types of recovery operations: Local recover and Directed recover. Local recovery implies a single NetWorker host that is both the backup source and recovery target. Directed recovery implies source and target machine are different.

NetWorker software is supported on various Operating Systems (OS), including:

- Microsoft
  - Windows XP SP3
  - Windows 7 SP1

[2] IT – Information Technology
[3] NDMP – Network Data Management Protocol
[4] NAS – Network Attached Storage

  - Windows Server 2003 SP2 and 2003 R2 SP2
  - Windows Server 2008 SP2 and 2008 R2 SP1
  - Windows Server 2012
- Unix-based
  - Solaris
  - AIX,
  - HP[5]-UX
- Linux-based
  - RedHat
  - SuSE
  - Oracle Enterprise Linux
  - CentOS
  - AsianUX
  - Debian
  - Fedora
  - Ubuntu
  - RedFlag
- Apple
  - Mac OSX
- Virtual Environments
  - VMware
  - Microsoft Hyper-V
  - Xen
  - Solaris Zones
  - IBM[6] LPARs[7]
  - HP VPARs[8]

NetWorker offers support for protection of several third-party applications through add-on application specific modules. These modules include support for the following applications:

- IBM DB2
- IBM Informix
- Lotus Notes
- Lotus Domino
- Oracle
- SAP[9]
- Sybase
- EMC Documentum
- MEDITECH
- Microsoft Active Directory
- Microsoft SharePoint
- Microsoft Exchange
- Microsoft SQL[10] Server
- Microsoft Data Protection Manager

NetWorker PowerSnap modules provide integration with EMC CLARiiON, EMC Symmetrix, and EMC RecoverPoint. NAS devices such as NetApp Data ONTAP and EMC Celerra DART are supported via native NDMP. NetWorker also works in concert with EMC Avamar and EMC Data Domain for client and

[5] HP – Hewlett Packard
[6] IBM – International Business Machines
[7] LPAR – Logical Partition
[8] VPAR – Virtual Partition
[9] SAP – System Analysis and Program Development, AG
[10] SQL – Structured Query Language

server-based deduplication. In addition, NetWorker supports virtual machine clients using traditional backup or using VMware Consolidated Backup (VCB).

EMC offers other tools to help manage configuration, such as a tool for managing configuration across multiple NetWorker servers, the License Manager tool for managing licensing across multiple EMC products or servers, as well as several optional add-on modules for SNMP[11], EMC DiskXtender, OpenVault, and EMC AutoStart.

1.3.1 NetWorker components

The NetWorker architectural model relies on client/server technology in which any client can interact with any server regardless of platform. The core NetWorker application is delivered to the customer as four components:

- NetWorker client
- NetWorker server
- NetWorker Management Console (NMC) server
- NetWorker storage node

1.3.1.1 NetWorker client

A NetWorker client is the collection of processes and programs installed on the machines that contain data to back up. The NetWorker client software communicates with the NetWorker server and provides client-initiated backup and recovery functionality. The NetWorker client software is installed on all computers that are backed up to the NetWorker server.

1.3.1.2 NetWorker server

A NetWorker server is the collection of processes and programs installed on the machine that organize and execute NetWorker functions. Each NetWorker server provides services for a datazone[12], including backup/recovery scheduling, queuing and coordination, and management of data lifecycles, volume pools, client indexes, and media databases.

The server coordinates backup operations, which 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. 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 to locate volumes required by operations and to automatically mount, unmount, and label those volumes as needed; to inventory autochangers; and to clone and stage data from one volume to another as requested.

1.3.1.3 NetWorker Management Console (NMC) server

The NMC server is the collection of processes and programs installed on the machine that performs NetWorker management console services. The NMC server is a Java-based web application server that provides centralized management, monitoring, and reporting of backup operations for multiple NetWorker servers and clients across multiple datazones. The NMC server is accessed through a graphical user interface (GUI) that can be run from any computer with a supported web browser and the Java Runtime Environment (JRE). Multiple users access the NMC server concurrently from different browser sessions.

[11] SNMP – Simple Network Management Protocol

[12] A NetWorker datazone is a single NetWorker server and its client and storage node computers.

1.3.1.4 NetWorker storage node

A NetWorker storage node is the collection of processes and programs installed on a remote machine with directly connected storage devices that is controlled by the NetWorker server. (Storage node software by default is installed with the NetWorker server, but can also be installed on a separate computer.)

Data is backed up directly to devices local to a NetWorker server or remotely 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 most of the data transfer involved in backup and recovery operations from the NetWorker server, improving overall performance.

1.3.2 NetWorker Methodology

As save sets are backed up and written to volumes, NetWorker relies on two data tracking databases: the client file index and the media database. The client file index is a browsable list of backed up files, organized by NetWorker client. The server updates the index with a new entry each time a file is backed up. Each entry includes the time of the backup, enabling users to identify specific versions of a backed up file. Entries remain in this browsable index for an administrator-defined period of time. NetWorker automatically removes entries from the client file index when the administrator defined "browse policy" for the client's data expires. The server updates the media database with an entry each time a save set is backed up and each time a storage volume is added to the NetWorker system. Entries remain in this database until they are manually removed by the administrator or the data on the volume is overwritten.

As data is written to storage, NetWorker tracks the data by volume and by the specific location that it is written on the volume, speeding up retrieval as necessary. An administrator can configure NetWorker in such a way that during backup, data is directed onto specific pools of volumes. Volume pools can be configured based on a variety of different data characteristics—data from similar clients can be written to the same pool, or data backed up at the same level. After data is written to a volume, NetWorker maintains information about the age of the data and automatically limits its recoverability, even eventually recycling the volume, based on administrator-defined data retention policies.

When data recovery is needed, users and administrators can browse an index of recoverable files, create reports that describe the status of data or the contents of the volumes, and recover data to a user-specified point in time. In response to a recovery request, the NetWorker storage management system locates the volume that contains the data and either directs a device to automatically mount the appropriate volume, or sends a message requesting the volume by name. If a site experiences a disaster, NetWorker can re-create all NetWorker client and server file systems to their original structure from a point in time when they were written to storage. NetWorker manages all volume operations including initial volume labeling, unmounting full volumes, requesting and mounting needed volumes, and volume relabeling and recycling.

The NetWorker storage model includes storage volumes, not specific devices. NetWorker backup and recovery is independent of the device or media type; that is, it is irrelevant whether the volumes that receive data are tapes, optical disk, or online disk. However, NetWorker only recognizes a volume within the context of a NetWorker pool of volumes. Administrators do not direct save sets either to a device or to a volume; they direct save sets to a named pool. In its most basic configuration, all NetWorker volumes would reside in a single pool and all save sets would be written to volumes in that pool.

1.4 TOE Overview

The TOE is a software-only backup and recovery solution that provides multi-tenancy and robust access control, authentication, auditing, confidentiality of backup sets using AES[13] encryption, and communication over secure TLS[14] channels. It is implemented as a collection of services on Windows and Linux based systems, as well as a collection of command line interfaces and GUIs, and a common

[13] AES – Advanced Encryption Standard
[14] TLS – Transport Layer Security

cryptographic provider library and wrapper. In general, an administrator can initiate all NetWorker functions either from within the GUI-based NMC Applet or from a set of NetWorker command-line and character-based interfaces. Additionally, end-users of client systems can perform ad-hoc backup and restore operations using a client GUI, known as the the NetWorker User interface. At boot time, NetWorker launches a number of services that run continuously on the server, client, and storage node machines. TOE user interfaces and services are described in section 1.4.1 below.

In general, the evaluated configuration of the TOE consists of five major components:

- NetWorker Server software running on a dedicated Windows Server 2008 R2 instance on GPC[15] hardware
- NetWorker Client software running in two separate instances on GPC hardware:
  - Windows Server 2008 R2
  - Linux
- NetWorker Storage Node software running on a dedicated Windows Server 2008 R2 instance on GPC hardware with an attached disk or tape device
- NMC Server software running on a dedicated Windows Server 2008 R2 instance on GPC hardware.
- NMC Applet running from a Java Virtual Machine within Internet Explorer 9 on a Windows 7 instance on GPC hardware

Figure 1 below shows the details of the deployment configuration of the TOE:

[15] GPC – General Purpose Computer

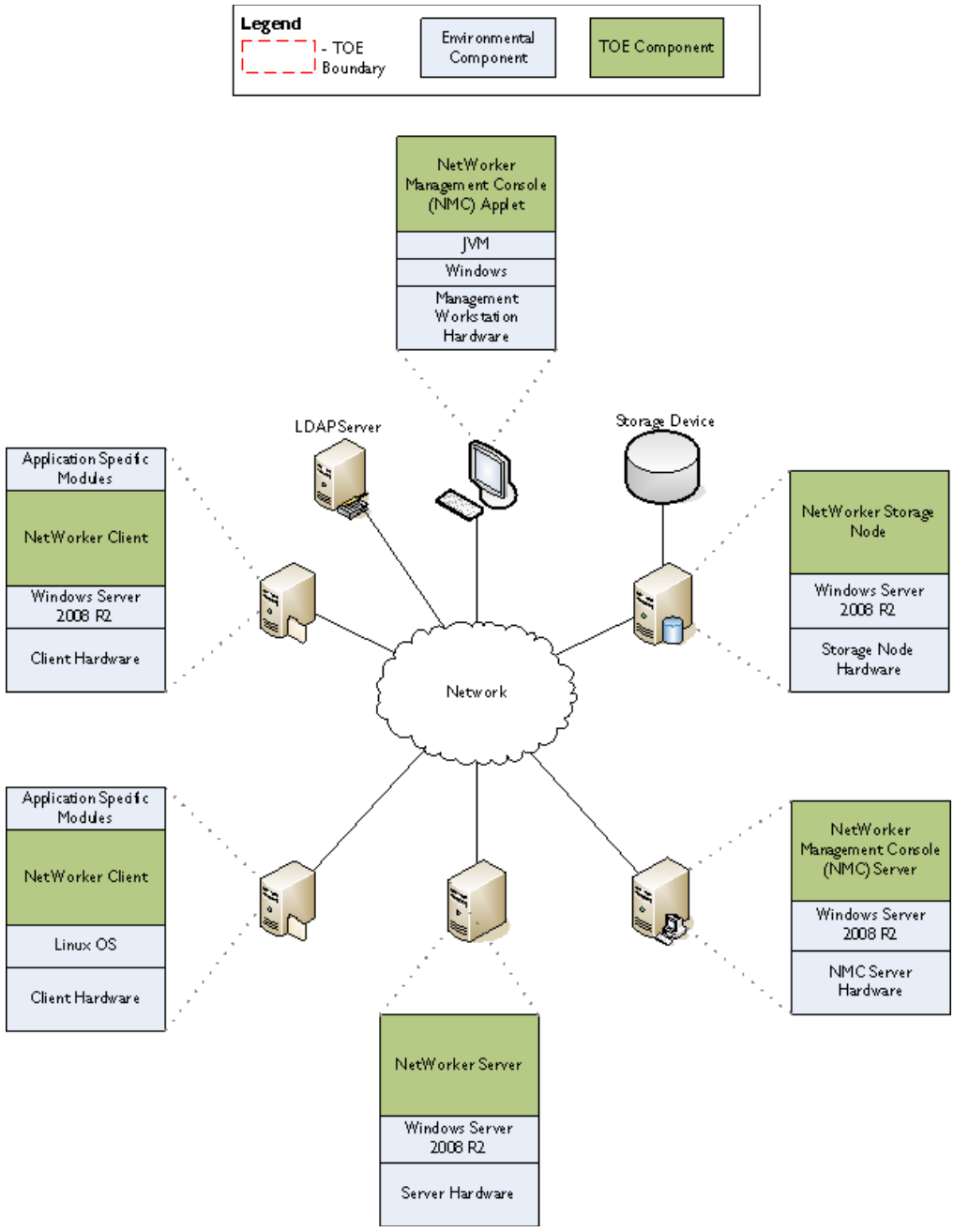

Figure 1 Deployment Configuration of the TOE[16][17]

[16] JVM – Java Virtual Machine

[17] The diagram above depicts a generic storage device attached to the NetWorker Storage Node. In the evaluated configuration, an Advanced File Type Device was used for testing.

1.4.1 Brief Description of the Components of the TOE

The NetWorker server is comprised of several services and applications, which include:

- **NetWorker Remote Exec Service** – This service authenticates and processes the NetWorker remote execution requests and executes utilities on the NetWorker server. This service also runs on NetWorker clients and storage nodes, as well as the NMC server.
- **NetWorker Backup and Recover Server Service** – This is the master service that controls other services on the NetWorker server, clients, and storage nodes. Controls all NetWorker activity on the server; including authorizing and coordinating save and recover operations, monitoring sessions, and compiling server statistics and messages. This service maintains the NetWorker configuration resource database.
- **NetWorker Media Management Database Service** – This service manages the NetWorker server's media database.
- **NetWorker Job Monitor** – This process monitors NetWorker activity during a backup or recovery operation.
- **NetWorker Index Management Service** – This is the service that manages the NetWorker server's online client file indexes. Provides a method for inserting entries into the client file index.
- **NetWorker Media Library Management Service** – This service provides media library management functions, providing an RPC-based service used to manage jukebox operations.
- **NetWorker Logging Service** – The logging service provides support for NetWorker audit logs and is configured to run on the NetWorker server by default.
- **NetWorker Character-based Interface** – Each NetWorker server includes a character-based interface that performs all the configuration functions found in the NMC.
- **NetWorker Server Command-line Interface** – Several command-line tools are provided with NetWorker server, which allow monitoring of the NetWorker server.

The NetWorker client consists of the following:

- **NetWorker Remote Exec Service** – This service authenticates and processes the NetWorker server remote execution requests and executes utilities on the client. The NetWorker client daemon is launched at boot time.
- **NetWorker User Interface –** The NetWorker User interface is a GUI-based application (Windows only) accessed by users of NetWorker client systems to perform ad-hoc backups and restores.
- **NetWorker Client Command-line Interface** – Several command-line tools are provided with NetWorker client, which provide backup, recovery, and monitoring operations for the NetWorker client.

The NetWorker storage node is comprised of the following services:

- **NetWorker Remote Exec Service –** This service authenticates and processes the NetWorker server remote execution requests and executes utilities on the storage node.
- **NetWorker Storage Node Media Management Service** – This service provides device support including labeling, multiplexing writes (interleaving data) to media during backups; demultiplexing reads (unweaving the data) from media during recovery; and generating requests for volume mounting and unmounting when appropriate..
- **NetWorker Storage Node Management Service** – This is an RPC[18]-based service used to manage all of the device operations that the NetWorker server media management service handles on behalf of the NetWorker Backup and Recover Server service on the NetWorker server. Ensures that the necessary device operations are performed as needed by the NetWorker Backup and Recover Server service.

[18] RPC – Remote Procedure Call

- **NetWorker Library Subsystem Service –** This service provides a uniform library interface to the NetWorker storage node media management service. Manages the library subsystem media, slot, drive, and port resources providing control to move and access the resources within the library subsystems.
- **NetWorker Storage Node Command-line Interface** – Several command-line tools are provided with NetWorker client, which allow management of the NetWorker storage node and devices.

The NMC server comprises the following:

- **NetWorker Remote Exec Service** – This service authenticates and processes NetWorker server remote execution requests.
- **Generic Services Toolkit (GST)** – The GST Controls other services provided by the NMC server.
- **Apache HTTP[19] Server 2.2.21** – The HTTP web server software provides the NMC Applet on the management workstation through a web browser.
- **Sybase SQL Anywhere 12.0.1** – The database server software manages information pertaining to the NMC.

The following software is executed from a separate management workstation:

- **NMC Applet** – This is a GUI-based Java applet used to interact with the NMC server to manage server, storage node, and client resources. This is the primary interface for management of the TOE. Although it is detailed in Figure 1 as running on the management workstation, it can be accessed from any client, server, or storage node using a standard web browser.

In addition to the services/interfaces described above, NetWorker uses the EMC LibcommonSSL library which wraps the FIPS 140-2 Validated RSA BSAFE library, which is used for control path (between NetWorker daemons) encryption, data path (backed-up data-at-rest) encryption, and protection of passwords. Also, each component integrates with the Common Security Toolkit (CST), which is bundled with the NetWorker product. CST provides a common interface to external authentication systems, as well as lockbox support, which provides protection of cryptographic keys, passwords, and configuration data.

1.4.2 TOE Environment

The essential required physical components for the TOE include:

- NetWorker server machine
- NetWorker client machine
- NetWorker storage node machine with attached disk or tape device
- NMC server machine
- Management workstation
- LAN[20] for network connectivity

In the evaluated configuration, the NetWorker server and NMC server run on Windows Server 2008 R2 SP1 and GPC hardware. The storage node runs on Windows Server 2008 R2 SP1 on a GPC with an attached disk or tape device. The NetWorker client is evaluated on two separate platforms: Microsoft Windows 2008 R2 SP1 and Red Hat Enterprise Linux 6 on GPC hardware. The management workstation runs on Windows 7 SP1 and GPC hardware. Also installed on the management workstation is the JRE 1.7, along with Internet Explorer 9, as needed to run the NMC Applet.

Table 2 specifies the minimum system requirements for the proper operation of the TOE.

[19] HTTP – Hypertext Transfer Protocol
[20] LAN – Local Area Network

Table 2 TOE Environment Minimum Requirements

Component	Requirement
NetWorker Server	OS: Microsoft Windows Server 2008 R2 SP1 CPU[21]: x64 compatible 1 GHz or greater RAM[22]: 8 GB[23] minimum Storage: 20 GB minimum
NetWorker Client	OS: Microsoft Windows Server 2008 R2 SP1 Red Hat Enterprise Linux 6 CPU: x64 compatible 1 GHz or greater RAM: 1 GB minimum Storage: 20 GB minimum
NetWorker Storage Node	OS: Microsoft Windows Server 2008 R2 SP1 CPU: x64 compatible 1 GHz or greater RAM: 1GB minimum Storage: 20 GB minimum Dedicated tertiary[24] storage device
NMC Server	OS: Microsoft Windows Server 2008 R2 SP1 CPU: x64 compatible 1 GHz or greater RAM: 1 GB minimum Storage: 20 GB minimum
Management Workstation (NMC Applet)	OS: Microsoft Windows 7 x64 SP1 CPU: x64 compatible 1 GHz or greater RAM: 1 GB minimum Storage: 20 GB minimum Software: JRE 1.7 Internet Explorer 9

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE included in the evaluation.

1.5.1 Physical Scope

The TOE is a distributed software-based application which runs on GPC hardware compliant to the minimum software and hardware requirements as listed in Table 2. The NetWorker client and server software support numerous operating system and hardware architecture combinations, but because the codebase for each of these platforms is very similar, only one Windows platform and one Linux platform are evaluated. The NetWorker software is supported on GPC workstations and servers, as well as several virtual environments; however virtual hypervisors are not evaluated.

The TOE boundary includes the NetWorker server binaries, the NetWorker storage node binaries, the NMC server binaries, and the NetWorker client binaries. The TOE also includes the NMC Java applet that executes in the browser of an administrator's workstation. The TOE boundary does not include licensable application modules such as those that facilitate integration with Microsoft SQL, Exchange, SharePoint, Oracle, SAP, Lotus Notes, etc, or any external storage systems. It also does not include the JRE, browsers,

[21] CPU – Central Processing Unit
[22] RAM – Random Access Memory
[23] GB – Gigabyte
[24] A tertiary storage device represents a tape drive, library, jukebox, or other device that handles mounts and dismounts for off-line storage media.

or the underlying operating systems and hardware platforms, nor does it include backup storage devices attached to the storage node.

The TOE is installed on a group of machines as depicted in Figure 2 below, which illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

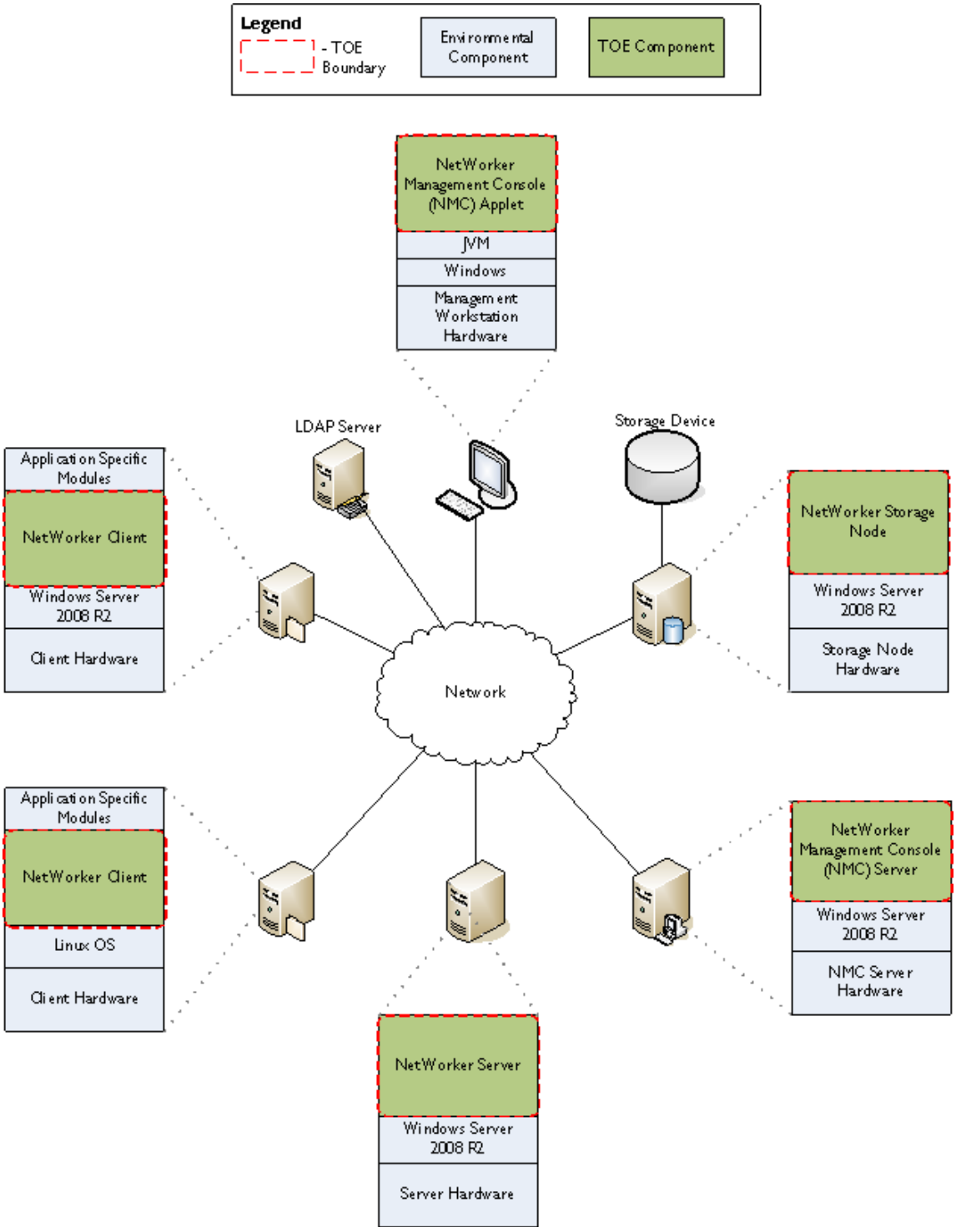

Figure 2 Physical TOE Boundary

1.5.2 Logical Scope

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE. The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[25]
- Resource Utilization
- TOE Access

1.5.2.1 Security Audit

The TOE provides robust auditing of client, server, and storage node operations, as well as security-relevant events occurring within the NMC. In addition, the TOE captures end-user actions including backup and recovery operations. Each NetWorker service records startup and shutdown events to the Windows Event Log.

Each recorded event includes a timestamp containing the date and time the event occurred, the event type, the identity of the subject who performed the action which caused the event, and the outcome of the event. In addition, each event also contains a severity level.

Each authenticated entity is provided with a unique identifier, which is permanent and persists across all NetWorker operations, allowing audit log events to be associated with a user. Two types of identifiers are used in NetWorker: User identifier and application identifier. The User identifier is used to identify the user performing NetWorker operations, while the application identifier is used to identify the source application performing a NetWorker operation.

The NetWorker server maintains the logging server, which collects events from all NetWorker resources within a datazone, preventing the loss of audit data storage on a failed resource. Audit logs are restricted to authorized users. The logging server also takes action to create a new file when the maximum file size has been reached. This value is initialized to 2 megabytes (MB).

1.5.2.2 Cryptographic Support

The TOE leverages the *libcommonSSL* library, which acts as a wrapper to the FIPS 140-2 validated BSAFE Crypto-C Micro Edition (ME) module, to support cryptographic operations. These include: symmetric encryption/decryption using AES, asymmetric encryption/decryption using RSA[26], signature generation/verification using RSA, hashing using SHA[27], and message authentication using HMAC[28]-SHA. Cryptographic keys are generated using a NIST[29] Special Publication (SP) 800-90 random bit generator. Manually entered keys are derived from user-defined pass phrases using the Password-Based Key Derivation Function. Keys are securely erased when no longer needed by the application.

The primary security functions for which the TOE requires cryptographic support include: lockbox pass phrase encryption, daemon-to-daemon TLS authentication, and client software-based encryption of backup data.

[25] TSF – TOE Security Functionality
[26] RSA – Rivest, Shamir, Adleman
[27] SHA – Secure Hash Algorithm
[28] HMAC – Hash-Based Message Authentication Code
[29] NIST – National Institute of Standards and Technology

1.5.2.3 User Data Protection

The TOE enforces the NetWorker Access Control SFP[30], which dictates the operations subjects may perform based on a set of security attributes. Subjects of the SFP include NMC users, NetWorker server users, and NetWorker daemons.

The TOE restricts NMC users from accessing specific console user interface elements and performing operations based on the user's role. Each role has a defined set of privileges with which it is associated. The NetWorker server restricts the operations that can be performed on the server, including management operations, as well as backup and recovery operations on NetWorker clients; these rights are based on the group to which a NetWorker server user belongs. Each group has an associated set of user privileges.

In addition to user authorization, each NetWorker host contains a server list which identifies the hosts that are allowed to perform client-tasking requests on behalf of NetWorker server users. Furthermore, each host maintains its own database of remote host public keys which it uses to authenticate requests from remote hosts. A user must possess the required privileges on the remote host in order to perform the requested actions.

The core functionality of the TOE involves user data backup and recovery. NetWorker supports scheduled backup operations in addition to manual backups. Backups may also be performed according backup groups, for a group of NetWorker clients that need to be backed up at the same time. Save sets identify the client resources to be backed up; these represent the collection of data items backed up during a backup session between the NetWorker server and the client resource.

In addition, the TOE provides recovery operations to roll back NetWorker client-protected computers to a previous state. Performing backup and recovery operations require sufficient privileges, which must be assigned by an administrator.

The TOE provides integrity of stored backup data by ensuring that backup data on the NetWorker server matches the data on the local disk. This feature compares the file types, file modification times, file sizes, and file contents, and alerts operators to any changes that have occurred to data since the backup. Verification also determines whether a hardware failure prevented the NetWorker server from completing a successful backup, and provides a way to test the ability to recover backup data.

To protect the confidentiality of backup data in transit and on tape or disk, the NetWorker client performs AES encryption on backup and archive data. The NetWorker client encrypts the data sent to the storage node, where it is transferred to a storage device. The backup data remains encrypted until a restore is requested. The encrypted backups are protected with the Datazone Encryption Key, which is encrypted using a user-defined Datazone Pass-Phrase.

1.5.2.4 Identification and Authentication

Identification and authentication functions deal with how a user's identity is asserted and subsequently verified by the TOE. NetWorker supports external authentication, which allows the TOE to be integrated with an existing LDAP[31] directory. During the NMC authentication process, password character feedback is obfuscated. Additionally, the NMC server echoes a message to the user after three failed authentication attempts, and upon acknowledgement, the NMC application is terminated.

When a user accesses the NMC, the user's credentials are passed to the remote LDAP server for verification. In addition to authentication, the LDAP server may be used for authorization. The TOE maintains a set of security roles, to which it maps a set of external roles, or LDAP groups. Subjects are bound to the security role for which an association has been established with an external role. If a user is not a member of any of the associated external roles, the NMC server denies the user access. Once a user is

[30] SFP – Security Function Policy
[31] LDAP – Lightweight Directory Access Protocol

authenticated to the NMC, they must possess the appropriate privilege on the NetWorker servers managed by the NMC in order to perform any NetWorker server operations.

The NetWorker User interface does not require end-user authentication prior to performing ad-hoc backup and recovery operations. Rather, it relies on authentication via the underlying OS facility. Once a user has been found to have a valid session, the TOE validates the user's authorization before allowing access to any privileged functions.

1.5.2.5 Security Management

Security Management functions define how the security functionality of the TOE is managed, the roles that are authorized to perform management functions, and the management of attributes that dictate the security functionality.

The NMC is the primary management interface for the TOE. It provides several functions for managing NetWorker resources, including NMC authentication, NetWorker server and client management, storage node, device, and media management, audit logs, backup and recovery operations, save sets, policies, schedules, etc., as well as reporting and monitoring of the overall NetWorker deployment.

The NMC supports the Console Security Administrator, Console Application Administrator, and Console User roles. In addition, each NetWorker server maintains authorization for client users based on user groups. The NetWorker server maintains the following user groups: Security Administrators, Application Administrators, Monitors, Operators, Auditors, Users, Database Operators, and Database Administrators.

Security attributes for TSF management functions, particularly those available to a Console Security Administrator or Security Administrator, are provided with secure default values. For example, new Console users are given Console User role privileges. When managing NetWorker server resources, new User Groups contain no privileges by default. Only the Console Security Administrator or Security Administrator may provide alternative values upon creation of a resource. In addition, NMC privileges do not automatically grant a user NetWorker server privileges, and vice versa. In order to access a NetWorker server managed through the NMC, the user must also be assigned the appropriate NetWorker server privileges via User Group membership.

1.5.2.6 Protection of the TSF

The TOE is capable of recovering from several types of disaster scenarios, including hardware failures, loss of network connectivity, and primary storage software failures. The NetWorker server backs up the NetWorker server and NMC server database on a regular schedule, allowing for the TOE to be restored to a secure state.

In the event of client software/hardware failure, or loss of network connectivity during a backup operation, the Checkpoint Restart feature is used to recover from a point of failure without the need to resave the entire save set. CheckPoint Restart allows a failed backup operation to restart at a known good point, prior to the point of failure.

TSF data transmitted between NetWorker server and client daemons is protected using a mutually authenticated, cryptographically secure channel. Each NetWorker daemon transmits TSF and user data through a TLS tunnel; the cryptographic functionally for which is provided *libcommonSSL* and the underlying RSA BSAFE Crypto-C ME module. Communication is initiated by a NetWorker client. (Note: NMC servers or NetWorker servers can also assume the role of a client, as they also contain NetWorker client binaries.) Each "server" maintains a list of certificates through which clients are authenticated to the server. The server and client communicate securely using an established TLS session using RSA for authentication, key exchange, and digital signing, AES for symmetric encryption, and HMAC-SHA for message authentication.

1.5.2.7 Resource Utilization

The TOE provides limited fault tolerance in the event of a failed backup operation; CheckPoint Restart backups allow a failed save operation to continue from the point of failure. Client backups are directed to the storage nodes. Therefore, in the event of a NetWorker server failure, clients continue to send backup data. However no new operations can take place until the NetWorker server is restored.

The TOE monitors its various services, including the storage node processes to ensure that they are functioning correctly. The NetWorker server periodically polls the status of the storage node, taking appropriate action, such as restarting a process, in the event of a failure. In addition, storage nodes can be configured as failover nodes in the event that the first node fails. Clients may also be assigned a node priority to instruct the client on which node it should transmit backup data to.

As a core feature of its backup and recovery features, NetWorker also provides browse and retention policies. A browse policy determines how long files are maintained in a client's index on the NetWorker server. A retention policy specifies the period of time which backed-up data is protected from accidental overwrite.

1.5.2.8 TOE Access

The NMC client displays a login banner prior to identification and authentication. The default text is "Warning: Authorized user only"; however the banner text is configurable by the Console Application Administrator.

1.5.3 Guidance Documentation

The following guides are required reading and part of the TOE:

- *EMC® NetWorker® Release 8.0 Service Pack 1 Administration Guide, P/N 300-999-719, REV A01*
- *EMC® NetWorker® Release 8.0 Service Pack 1 Command Reference Guide, P/N 300-999-721, REV A01*
- *EMC® NetWorker® Release 8.0 Service Pack 1 Error Message Guide, P/N 300-999-724, REV A01*
- *EMC® NetWorker® Release 8.0 Service Pack 1 Installation Guide, P/N 300-999-725, REV A01*
- *EMC® NetWorker® Release 8.0 and Service Packs Release Notes, P/N 300-013-567, REV A05, December 14, 2012*
- *EMC® NetWorker® 8.0 Cumulative Hotfixes, April 2013*
- *EMC® NetWorker® 8.0.1.4 Guidance Documentation Supplement v0.4*

1.5.4 Product Physical/Logical Features and Functionality not included in the TSF

Features and Functionality that are not part of the evaluated configuration of the TOE are:

- Native NMC authentication
- Data Domain Integration
- Avamar Integration
- NetWorker Autochanger Module
- NetWorker Silo Software Module
- NetWorker Archive Module
- NetWorker Database Modules
- NetWorker SNMP
- NetWorker NDMP support
- EMC DiskXtender Data Manager File System Support
- Support for OpenVault remote storage systems (Windows only)

- Cluster support, including EMC AutoStart software
- NetWorker License Manager
- Advanced reporting capability
- NetWorker Client Push service
- *nwrecover* Client Interface for Unix/Linux

2 Conformance Claims

This section and Table 3 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 3 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM[32] as of 2012/10/22 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ augmented with Flaw reporting procedures (ALC_FLR.2)

[32] CEM – Common Evaluation Methodology

3 Security Problem

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment
- Organizational security policies with which the TOE must comply
- Assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects

3.1 Threats to Security

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not TOE users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters and no physical access to the TOE.
- TOE users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters and physical access to the TOE. (TOE users are, however, assumed not to be willfully hostile to the TOE.)
- Environmental conditions: Conditions or forces external to the TOE that may adversely affect hardware; e.g. power outages, faulty hardware components, disasters, etc.

Both are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 4 below lists the applicable threats.

Table 4 Threats

Name	Description
T.COMPROMISE	Critical system or user data may be compromised due to a failure, rendering data unusable. Threat agent is an environmental condition or force that results in hardware failure.
T.DATALOSS	Backups of critical system or user data may be overwritten, modified, or accessed by an unauthorized user.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.TAMPERING	A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.
T.UNAUTH	A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.
T.WEAKCRYPTO	An unauthorized user may exploit a weakness in a protocol or algorithm to gain access to sensitive information handled by the TOE.

3.2 Organizational Security Policies

An Organizational Security Policy (OSP) is a set of security rules, procedures, or guidelines imposed by an organization on the operational environment of the TOE. Table 5 below lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

Table 5 Organizational Security Policies

Name	Description
P.MANAGE	The TOE may only be managed by authorized users.
P.INTEGRITY	Data collected and produced by the TOE must be protected from modification.

3.3 Assumptions

This section describes the security aspects of the intended environment for the evaluated TOE. The operational environment must be managed in accordance with assurance requirement documentation for delivery, operation, and user guidance. Table 6 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 6 Assumptions

Name	Description
A.INSTALL	The TOE is installed on the appropriate, dedicated hardware and operating system.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.LOCATE	The TOE, and all TSF-dependent services, including the LDAP server used for authentication and authorization, are located within a secure, controlled access facility.
A.NOEVIL	The users who manage the TOE, and the TSF-dependent services in the IT Environment, are non-hostile, appropriately trained, and follow all guidance.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.

4 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see Section 3). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 7 below.

Table 7 Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.
O.AUDIT	The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.
O.AUTHENTICATE	The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.
O.BACKUP	The TOE must protect user data by implementing a backup and recovery mechanism that ensures integrity, availability, and confidentiality of backup data.
O.CRYPTO	The TOE must incorporate a FIPS 140-2 validated module that provides approved functions for key generation, destruction, and cryptographic operations.
O.PROTECT	The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 8 below lists the IT security objectives that are to be satisfied by the environment.

Table 8 IT Security Objectives

Name	Description
OE.PLATFORM	The TOE hardware and OS must support all required TOE functions.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.

4.2.2 Non-IT Security Objectives

Table 9 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 9 Non-IT Security Objectives

Name	Description
OE.MANAGE	Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.
OE.PHYSICAL	The physical environment must be suitable for supporting a computing device in a secure setting.

5 Extended Components

This section defines the extended SFRs and extended SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

5.1 Extended TOE Security Functional Components

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 10 identifies all extended SFRs implemented by the TOE

Table 10 Extended TOE Security Functional Requirements

Name	Description
EXT_FRU_DRP.1	Minimum retention lock periods

5.1.1 Class FRU: Resource Utilization

Resource Utilization functions involve the guaranteed availability of required resources such as processing capability and/or storage capacity. It does not however, specify families of requirements for data retention. As a result, the extended family and related components for EXT_FRU_DRP: Retention lock periods was created, and is modeled after the CC family FRU_RSA: Resource allocation.

5.1.1.1 Data retention periods (EXT_FRU_DRP)

Family Behaviour

The requirements of this family allow the TSF to control the use of data retention periods.

Component Leveling

Figure 3 EXT_FRU_DRP Data retention periods family decomposition

EXT_FRU_DRP.1 Minimum retention lock periods, provides the capability to institute retention periods for the purpose of protecting a file from being modified or deleted during the specified retention period.

Management: EXT_FRU_DRP.1

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

- Specifying minimum retention lock periods for specified files.

Audit: EXT_FRU_DRP.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Rejection of file modification or deletion attempt due to active retention lock period.
- Basic: All attempted file modifications or deletions for files that are under control of the TSF.

EXT_FRU_DRP.1 Minimum retention lock periods
Hierarchical to: No other components
EXT_FRU_DRP.1.1

The TSF shall enforce minimum retention lock periods of files of stored user data that are retained on backup media in a non-rewriteable and non-erasable format.

Dependencies: No dependencies

5.2 Extended TOE Security Assurance Components

No extended assurance components are included in this ST.

6 Security Requirements

This section defines the SFRs and SARs met by the TOE. These requirements are presented following the conventions identified in Section 6.1.

6.1 Conventions

There are several font variations used within this ST. Selected presentation choices are discussed here to aid the Security Target reader.

The CC allows for assignment, refinement, selection and iteration operations to be performed on security functional requirements. All of these operations are used within this ST. These operations are performed as described in Part 2 of the CC, and are shown as follows:

- Completed assignment statements are identified using *italicized text*.
- Completed selection statements are identified using underlined text.
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Extended Functional and Assurance Requirements are identified using "EXT_" at the beginning of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 11 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 11 TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_GEN.2	User identity association				
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.3	Action in case of possible data loss		✓		
FCS_CKM.1	Cryptographic key generation		✓		
FCS_CKM.4	Cryptographic key destruction		✓		
FCS_COP.1	Cryptographic operation		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_ITT.1	Basic internal transfer protection	✓	✓		
FDP_ROL.2	Advanced rollback		✓		
FDP_SDI.1	Stored data integrity monitoring		✓		
FIA_AFL.1	Authentication failure handling	✓	✓		

Name	Description	S	A	R	I
FIA_UAU.1	Timing of authentication		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MOF.1	Management of security functions behaviour	✓	✓	✓	
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		✓		
FRU_FLT.1	Degraded fault tolerance		✓		
EXT_FRU_DRP.1	Minimum retention lock periods				
FPT_ITT.1	Basic internal TSF data transfer protection	✓			
FPT_FLS.1	Failure with preservation of secure state		✓		
FTA_TAB.1	Default TOE access banners				

Note: S=Selection; A=Assignment; R=Refinement; I=Iteration

6.2.1 Class FAU: Security Audit

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) *NetWorker daemon events, NMC server events, User events, and Application 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*.

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.

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.

FAU_STG.3 Action in case of possible audit data loss
Hierarchical to: No other components.
Dependencies: FAU_STG.1 Protected audit trail storage
FAU_STG.3.1

The TSF shall *take action to rename and archive the security audit log file* if the audit trail exceeds *2 MB*.

6.2.3 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation
Hierarchical to: No other components.
Dependencies: 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 *Digital Signature Standard (DSS) pseudorandom number generator (PRNG), Dual Elliptic Curve (EC) Deterministic Random Bit Generator (DRBG), Hash-based Message Authentication Code (HMAC) DRBG, Password-Based Key Derivation Function 2 (PBKDF2)* and specified cryptographic key sizes *cryptographic key sizes defined in FCS_COP.1* that meet the following: *FIPS 186-2, NIST SP 800-90A, and NIST SP 800-132*.

FCS_CKM.4 Cryptographic key destruction
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation

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*.

FCS_COP.1 Cryptographic operation
Hierarchical to: No other components.
Dependencies: FCS_CKM.1 Cryptographic key generation
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1

The TSF shall perform *symmetric encryption/decryption, asymmetric encryption/decryption, key generation, random bit generation, signature generation/verification, hashing, and message authentication* in accordance with a specified cryptographic algorithm *defined in Table 12 below* and cryptographic key sizes *defined in Table 12 below* that meet the following: *standards defined in Table 12 below*.

Table 12 Cryptographic Algorithms

Algorithm	Key Size	Standard	Certificate No.
AES ECB[33], CBC[34], CFB[35]-128, OFB[36]-128, CTR[37], CCM[38], GCM[39], and GMAC[40]	*EBC, CBC, CTR, CCM, GCM, and GMAC: 128, 192, and 256-bit* *CFB and OFB: 128-bit*	*FIPS 197*	810, 860, 1771, 1951 GCM and GMAC vendor affirmed
Triple-DES[41] ECB, CBC, CFB, and OFB	*ECB and CBC:* *CFB and OFB: 64-bit*	*NIST SP 800-67*	690, 707, 1147, 1268
Diffie-Hellman, EC-Diffie-Hellman	*between 112 and 150-bit*		Non-approved

[33] ECB – Electronic Codebook
[34] CBC – Cipher Block Chaining
[35] CFB – Cipher Feedback
[36] OFB – Output Feedback
[37] CTR – Counter
[38] CCM – Counter with CBC-MAC
[39] GCM – Galois Counter Mode
[40] GMAC – Galois Message Authentication Code
[41] DES – Data Encryption Standard

Algorithm	Key Size	Standard	Certificate No.
DSA[42], EC-DSA	*2048-bit*	*FIPS 186-3*	DSA: 300, 311, 554, 623 EC-DSA: 92, 93, 98, 100, 239, 240, 281, 282
RSA X9.31, PKCS[43] #1 v1.5, and PKCS #1 v2.1	*between 1024 and 4096-bit in multiples of 512*	*RSASSA[44]-PKCS#1 v1.5* *RSASSA-PSS[45]*	390, 412, 887, 1012
RSA encrypt and decrypt	*RSA key wrap: between 112 and 150-bit*	*RSASSA-PKCS#1 v1.5*	Allowed for key transport
FIPS 186-2 PRNG		*FIPS 186-2*	466, 492, 943, 1027
Dual EC-DRBG and HMAC-DRBG		*NIST SP 800-90A*	2, 4, 122, 172
PBKDF2		*NIST SP 800-132*	Non-approved
SHA-1, 224, 256, 384, 512		*FIPS 180-4*	807, 855, 1555, 1713
HMAC-SHA-1, 224, 256, 384, 512	*between 112 and 4096*	*FIPS 198-1*	449, 477, 1040, 1177

[42] DSA – Digital Signature Algorithm
[43] PKCS – Public Key Cryptography Standard
[44] RSASSA – RSA Signature Scheme with Appendix
[45] PSS – Probabilistic Signature Scheme

6.2.4 Class FDP: User Data Protection

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 *NetWorker access control SFP* on

a. *Subjects: users accessing NMC console, users accessing NetWorker server, and NetWorker components accessing other NetWorker components*
b. *Objects: NMC user interface elements, user data, and TSF data*
c. *Operations:*
    i. *NMC server:*
        1. *Add, modify, delete NMC users;*
        2. *Configure login authentication;*
        3. *Control access to managed applications;*
        4. *Configure system options;*
        5. *Set retention policies;*
        6. *View reports;*
        7. *Backup NMC database;*
        8. *Configure NetWorker License Manager;*
        9. *Configure NMC options;*
        10. *Add/delete hosts and folders;*
        11. *Add/delete managed applications;*
        12. *Create/delete reports;*
        13. *Configure managed application features;*
        14. *Manage NetWorker server;*
        15. *Dismiss events;*
    ii. *NetWorker server*
        1. *Create, view, modify, delete User groups;*
        2. *Change/view security settings (Audit Log resource, server settings);*
        3. *Remotely browse and recover client data;*
        4. *View client resource configurations;*
        5. *Configure NetWorker server, storage nodes, and clients;*
        6. *Monitor NetWorker operations;*
        7. *View media database information;*
        8. *View NetWorker configuration information;*
        9. *Operate devices and jukeboxes;*
        10. *Recover local client data;*
        11. *Backup local client data;*
        12. *Create, View, Change, Delete application settings;*
        13. *Archive data;*
        14. *Backup remote client data;*
        15. *Recover remote client data;*
    iii. *All NetWorker Components*
        1. *Client-Tasking*
        2. *Store, retrieve, and delete lockbox passwords*
        3. *Encrypt/decrypt backups*

Application Note: *The "NetWorker server" management functions described in item c.ii above represent the actions which can be performed on a NetWorker server by an administrator through the NMC; however, the enforcement of the NetWorker Access Control SFP with respect to NetWorker servers is unique to each instance of the NetWorker server. For example, NMC console access does not*

implicitly grant access to individual NetWorker servers. In order to perform the management functions described above, the user must be afforded privileges through membership of NetWorker server user groups, which are maintained independently by each NetWorker server.

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 initialization

FDP_ACF.1.1

The TSF shall enforce the *NetWorker access control SFP* to objects based on the following:

a) *Subjects:*
   a. *Users accessing NMC*
      i. *Security Attributes:*
         1. *User Name*
         2. *User Role (security role)*
         3. *Role Privileges*
   b. *Users accessing NetWorker server*
      i. *Security Attributes*
         1. *User Name*
         2. *User Group*
         3. *Group Privileges*
   c. *NetWorker components accessing other NetWorker components*
      i. *Security Attributes*
         1. *Authentication keys*
         2. *Session keys*
         3. *Session ID*[46]
         4. *User Information*
         5. *User Privileges*

b) *Objects:*
   a. *NetWorker components*
      i. *Security Attributes*
         1. *Client-Tasking Rights*
         2. *User Name (lockbox pass phrase access)*
         3. *Datazone Pass Phrase*

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

- *A user may only interact with NMC elements to which the user's role permits access based on the role's privileges.*
- *A user may only interact with NetWorker servers to which the user's group permits access based on the group's privileges.*
- *A NetWorker component may only communicate with another NetWorker component if the two components are mutually authenticated.*
- *A NetWorker component may access and perform operations on other NetWorker components on behalf of the requesting user if the requesting component has been given client-tasking rights in the target component's server file, or if no components are listed in a component's server file.*
- *A NetWorker component can act on another NetWorker component on behalf of the requesting user only if the user carries the appropriate privileges on the target component.*
- *A user can access lock box contents (Datazone Encryption Key, passwords, etc.) only if the user has been granted access to the lockbox.*

[46] ID - Identifier

- *A user can decrypt lock box contents (Datazone Encryption Key, passwords, etc.) only if the user knows the Datazone Pass Phrase.*

FDP_ACF.1.3

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: *none*.

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the *none*.

FDP_ITT.1 Basic internal transfer protection

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control

FDP_ITT.1.1

The TSF shall enforce the *NetWorker access control SFP* to prevent the disclosure, modification of user data when it is transmitted between physically-separated parts of the TOE.

FDP_ROL.2 Advanced rollback

Hierarchical to: FDP_ROL.1 Basic rollback

Dependencies: FDP_ACC.1 Subset access control

FDP_ROL.2.1

The TSF shall enforce *NetWorker access control SFP* to permit the rollback of all the operations on the *NetWorker clients, NetWorker server, and NMC server*.

FDP_ROL.2.2

The TSF shall permit operations to be rolled back within the *capabilities and limitations of backup data sets, as defined by the browse and retention policies*.

FDP_SDI.1 Stored data integrity monitoring

Hierarchical to: No other components

Dependencies: No dependencies

FDP_SDI.1.1

The TSF shall monitor user data stored in containers controlled by the TSF for *integrity errors* on all objects, based on the following attributes: *file types, file modification times, file sizes, and file contents*.

6.2.5 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication
FIA_AFL.1.1

The TSF shall detect when *three* unsuccessful authentication attempts occur related to *NMC authentication*.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been *met*, the TSF shall *display a message indicating that the maximum number of attempts has been exceeded and, upon acknowledgement of the message, terminate the application*.

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification
FIA_UAU.1.1

The TSF shall allow *client backups and restores* on behalf of the user to be performed before the user is authenticated.

FIA_UAU.2

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

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 *obfuscated character feedback* to the user while the authentication is in progress.

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.

6.2.6 Class FMT: Security Management

FMT_MOF.1 Management of security functions behaviour
Hierarchical to: No other components.
Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF.1.1

The TSF shall restrict the ability to **take the actions listed in Table 13 on** the functions *listed in Table 13* to *the roles listed in Table 13*.

Table 13 Management of Security Functions Behavior

Action	Function	Role
NMC server		
Determine the behavior of, modify the behavior of	*User authentication*	*Console Security Administrator*
	Access control	
Determine the behavior of, modify the behavior of	*Console system options*	*Console Application Administrator*
	TSF data backup	
	Console configuration	
Determine the behavior of, modify the behavior of	*Clients and client resources*	*Console Security Administrator* *Console Application Administrator* *Console User*
	Managed applications	
	NetWorker server	
NetWorker server		
Determine the behavior of, modify the behavior of	*Security settings*	*Security Administrator*
Determine the behavior of, modify the behavior of	*NetWorker server*	*Application Administrator*
	NetWorker clients	
	Backups	
	Application settings	
Determine the behavior of	*NetWorker server*	*Monitor*
	Backups	
	Application settings	
	Security Settings	
Modify the behavior of	*Backups*	*Monitor*
Determine the behavior of	*NetWorker server*	*Operator*
	NetWorker clients	
	Backups	
	Application settings	
Modify the behavior of	*Backups*	*Operator*

Action	Function	Role
	NetWorker clients	
Determine the behavior of	*Security settings*	*Auditor*
Determine the behavior of	*Backups*	*User*
	NetWorker server	
Modify the behavior of	*Backups*	*User*
Determine the behavior of	*NetWorker server*	*Database Operator*
	NetWorker clients	
	Backups	
Modify the behavior of	*NetWorker clients*	*Database Operator*
	Backups	
Determine the behavior of, modify the behavior of	*NetWorker server*	*Database Administrator*
	NetWorker clients	
	Backups	

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.1.1

The TSF shall enforce the *NetWorker access control SFP* to restrict the ability to **perform the operations listed in Table 14 on** the security attributes *identified in Table 14* to *the roles identified in Table 14*

Table 14 Management of Security Attributes

Operation	Attributes	Roles
NMC server		
Query	*User Name*	*Console User* *Console Application Administrator* *Console Security Administrator*
	Last Login/Logout Time	
	Console System Options	
Query	*Host Permissions*	*Console Application Administrator* *Console Security Administrator*
	Certificates	
Delete	*Certificates*	*Console Application Administrator* *Console Security Administrator*
Modify	*Console System Options*	*Console Application Administrator* *Console Security Administrator*
	Console Configuration Options	
Query	*Authentication Method*	*Console Security Administrator*
	LDAP Attributes	

Operation	Attributes	Roles
Modify, delete	*User Name*	*Console Security Administrator*
	Host Permissions	
	LDAP Attributes	
Change default	*Authentication Method*	*Console Security Administrator*
NetWorker server		
Query	*User Groups*	*Security Administrator* *Auditor* *Monitor*
	Audit Log resource	
	NetWorker Server resource	
Modify, delete	*User Groups*	*Security Administrator*
	Audit Log resource	
	NetWorker Server resource	
Query	*Client resources*	*Application Administrator* *Operator* *Database Operator* *Database Administrator*
Query	*NetWorker server, storage node, and client resources*	*Security Administrator* *Application Administrator* *Database Operator* *Database Administrator* *Operator* *User* *Auditor* *Monitor*
Modify, delete	*NetWorker server, storage node, and client resources*	*Security Administrator* *Application Administrator* *Database Administrator* *Monitor*
Query	*Archive Requests*	*Application Administrators* *Monitor* *Operator*
	Device resources	
	Directives	
	Group	
	Jukebox	
	Label	
	License	
	Notification	
	Policies	
	Schedule	
	Staging	
	Storage Node	

Operation	Attributes	Roles
Modify, delete	*Archive Requests*	*Application Administrator*
	Device resources	
	Directives	
	Group	
	Jukebox	
	Label	
	License	
	Notification	
	Policies	
	Schedule	
	Staging	
	Storage Node	

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 *NetWorker 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 *Console Security Administrators, Security Administrators* to specify alternative initial values to override the default values when an object or information is created.

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: *User/authentication management, access control management, audit log management, server, client, and storage node management, console management, application management, and client backup management*.

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 *Console Security Administrators, Console Application Administrators, Console Users, Security Administrators, Application Administrators, Monitors, Operators, Auditors, Users, Database Operators, Database Administrators*.

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.8 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: *hardware failures, loss of network connectivity, and primary storage software failures*.

FPT_ITT.1 Basic internal TSF data transfer protection
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_ITT.1.1

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE.

6.2.9 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance
Hierarchical to: No other components.
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1

The TSF shall ensure the operation of *backup operations* when the following failures occur: *hardware failure, loss of network connectivity, and primary storage software failure*.

EXT_FRU_DRP.1 Minimum retention lock periods
Hierarchical to: No other components
EXT_FRU_DRP.1.1

The TSF shall enforce minimum retention lock periods of files of stored user data that are retained on backup media in a non-rewriteable and non-erasable format.

Dependencies: No dependencies

6.2.10 Class FTA: TOE Access

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.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2 augmented with ALC_FLR.2. Table 15 Assurance Requirements summarizes the requirements.

Table 15 Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	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
Class ALC : Life Cycle Support	ALC_CMC.2 Use of a CM[47] system
	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw reporting procedures
Class ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[47] CM – Configuration Management

7 TOE Security Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security function. Hence, each security function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 16 lists the security functionality and their associated SFRs.

Table 16 Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User identity association
	FAU_STG.1	Protected audit trail storage
	FAU_STG.3	Action in case of possible data loss
Cryptographic Support	FCS_CKM.1	Cryptographic key generation
	FCS_CKM.4	Cryptographic key destruction
	FCS_COP.1	Cryptographic operation
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_ITT.1	Basic internal transfer protection
	FDP_ROL.2	Advanced rollback
	FDP_SDI.1	Stored data integrity monitoring
Identification and Authentication	FIA_AFL.1	Authentication failure handling
	FIA_UAU.1	Timing of authentication
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MOF.1	Management of security functions behaviour
	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

TOE Security Function	SFR ID	Description
Protection of TOE Security Functions	FPT_ITT.1	Basic internal TSF data transfer protection
	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
	EXT_FRU_DRP.1	Minimum retention lock periods
TOE Access	FTA_TAB.1	Default TOE access banners

7.1.1 Security Audit

The Security Audit functions define how the TOE generates an audit trail of security-relevant activities, including the types of events generated and the types of information contained within an audit event. It also defines how the TOE protects the integrity and prevents the loss of stored audit data.

The TOE maintains a separate security audit trail that is used to track security relevant transactions. The main purpose of the TOE's audit function is to record all the attempts to modify critical system configurations. This includes changes to users, groups, and devices, whether the attempt is successful or not. The audit report includes changes prompted by the user requests, including changes to attribute values and the creation and deletion of resources.

Each authenticated entity is provided with a unique identifier, which is permanent and persists across all NetWorker operations, allowing audit log events to be associated with a user. Two types of identifiers are used in NetWorker: User identifier and application identifier. The User identifier is used to identify the user performing NetWorker operations, while the application identifier is used to identify the source application performing a NetWorker operation.

Security auditing is handled by the daemon logging process, which runs on the NetWorker server. Within the TOE deployment, a NetWorker server and its clients define a datazone. The logging server is a defined client of the NetWorker datazone. Each datazone has one logging server. A single logging server may also support multiple datazones. The logging server is responsible for logging security messages from any NetWorker computer within a single datazone. Only those computers that are configured by the NetWorker server may log messages to the logging server. By default, the logging service runs on the NetWorker server; however, it can be configured to run on any NetWorker client. Only a user who has the Security Administrator Role can modify the logging server behavior.

The security audit function records the following types of events:

- Operations that require authorization
- Attempts to modify critical system configurations

These audit events are captured in the audit log file and are configurable to meet the end user security policy. In addition, startup and shutdown events are recorded for each of the daemons that comprise the TOE. Audited events also include a severity level, which may be used to set the verbosity of logging. Severity levels include: DEBUG, INFO, NOTICE, WARNING, INTERVENTION, ERROR, SEVERE, CRITICAL, ALERT, and EMERGENCY.

In addition to the events logged by the logging server, the NMC logs these auditable events:

- Creation/Update/Deletion of the user in NMC.
- Addition/Deletion of NetWorker server hosts to NMC Enterprise Hierarchy.
- Addition/Deletion of Managed Application to NMC Enterprise Hierarchy.

- Modification of "Capture Events", "Gather Reporting Data" features of a host.
- Modification of System Options.
- Reset of NMC database connection credentials.
- Changes to NMC Console Configuration settings.

The TOE prevents unauthorized modifications to the audit trail. No methods are provided to the end users for deleting/modifying audit records. Furthermore, the audit log file cannot be accessed while while the TOE is running, as it is locked by the logging daemon when in use. A command line utility may be used to render audit logs for administrator review; however the utility only provides read access to the audit entries.

The logging server rotates log files based on a maximum file size, which is initialized to 2 MB. The logging daemon monitors the size when the file is opened and on a periodic basis (every 100th write). When this size is exceeded (plus or minus 1%), the file is copied to a backup file with file name extension .1, or the first unused number if .1 already exists.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_STG.1, FAU_STG.3.

7.1.2 Cryptographic Support

The cryptographic support functions define all cryptographic operations, key generation, and destruction methods. The TOE employs a FIPS 140-2 validated module for all cryptographic functionality, which includes lockbox pass phrase encryption, daemon-to-daemon TLS authentication, and client software-based encryption of backup data. The primitives for these cryptographic operations are provided by the RSA BSAFE Crypto-C Micro Edition 3.0.0.1 (Certificate #1092) library.

Credentials for NetWorker client resources are stored in an AES-256 encrypted lockbox, which is protected using the Datazone pass phrase. This user-defined pass phrase is converted to the Datazone key using PBKDF2. The Datazone key is also used to perform encryption and decryption of backups for clients within a Datazone. Encryption and decryption of backup data occurs at the NetWorker client; the resulting effect is that the backup data is protected in transit and remains protected when backed up to tape or disk.

Communications between NetWorker daemons are protected using an authenticated TLS session. Upon initial registration of a NetWorker client with the server, the NetWorker Remote Exec service generates a public RSA key pair along with a self-signed X.509 certificate. These key pairs are used to authenticate NetWorker daemons and establish a TLS session. TLS session data is encrypted using AES-128, and authenticated with an HMAC key. The information transmitted over this secure connection includes session keys, session ID, user information, and user rights.

While the primary cryptographic functionality of the TOE is highlighted above, the RSA BSAFE Crypto-C ME module supports several Approved functions. These include:

- AES ECB, CBC, CFB-128, OFB-128, CTR (128, 192, and 256-bit key sizes), and CCM
- AES GCM (128, 192, 256-bit key sizes) and GMAC (129, 192, and 256-bit key sizes)
- Triple-DES ECB, CBC, CFB (64-bit), and OFB (64-bit)
- Diffie-Hellman, EC-Diffie-Hellman, and EC-Diffie-Hellman with Components
- DSA
- ECDSA
- FIPS 186-2 PRNG
- Dual EC-DRBG and HMAC-DRBG
- RSA X9.31, PKCS#1 V1.5, and PKCS#1 V2.1
- RSA encrypt and decrypt
- SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512

- HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512

The operating system protects memory and process space from unauthorized cryptographic key access. Keys are subsequently zeroized when they are no longer required.

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

7.1.3 User Data Protection

The TOE enforces the NetWorker Access Control SFP, which dictates the operations subjects may perform based on a set of security attributes. Subjects of the SFP include NMC users, NetWorker server users, and NetWorker daemons.

The TOE restricts NetWorker Management Console users from accessing specific console user interface elements and performing operations based on the user's role. Each role has a defined set of privileges with which it is associated.

The NetWorker server restricts the operations which can be performed on the server, including management operations, as well as backup and recovery operations on NetWorker clients; these rights are based on the group to which a NetWorker server user belongs. Each group has an associated set of user privileges. Users must be added to the appropriate user group on the appropriate NetWorker server in order to access NetWorker resources. By default, the Windows System account, Administrator account, and Administrators group are added to the NetWorker server Administrators user group.

In addition to user authorization, each NetWorker host contains a server list which identifies the hosts which are allowed to perform client-tasking requests on behalf of NetWorker server users. Furthermore, each host maintains its own database of remote host public keys which it uses to authenticate requests from remote hosts. A user must possess the required privileges on the remote host in order to perform the requested actions.

The core functionality of the TOE involves user data backup and recovery, allowing the client-protected machines to be rolled back to a previous state for which the TOE has valid backup sets. NetWorker provides protection of file system data and application data for clients, servers, storage nodes, and the NMC server. The recovery capabilities are dependent on an active backup schedule; e.g. in order to roll back a NetWorker client system, there must be a recent backup available which reflects the system state prior to the operations that the TOE user wishes to roll back. In addition, the backup must be within the current retention period defined for the client in order to guarantee availability of the backup data. For users performing restores through the NetWorker User application, the backup must be within the browse period defined for the client; otherwise, the backup media requires a re-index.

Performing backup and recovery operations require sufficient privileges; for example, a user must be a part of a NetWorker server user group that has the "Recover Local Data" privilege. To back up a remote NetWorker host, the user must be part of a group that has the "Backup Remote Data" privilege. Table 17 explains the NetWorker server privileges. NMC server privileges are discussed in further detail in section 6.2.6.

Table 17 NetWorker Server Privileges

NetWorker Privilege	Allowed Operations
Change security settings	The ability to modify: • User groups • The Audit Log resource • The server resource

NetWorker Privilege	Allowed Operations
View security settings	The ability to view: • User groups • The Audit Log resource • The server resource.
Create security settings	The ability to create new user group resources.
Delete security settings	The ability to delete user created user groups. Preconfigured user groups cannot be deleted.
Remote access all clients	The ability to: • Remotely browse and recover data associated with any client • View configurations for all Client resources. This privilege is required to perform Directed Recovers.
Configure NetWorker	The ability to configure resources associated with the NetWorker server, storage nodes, and clients. This includes creating, editing, and deleting resources. Users with this privilege cannot configure User Group resources.
Operate NetWorker	The ability to perform NetWorker operations. For example, members can: • Reclaim space in a client file index. • Set a volume location or mode. • Start or stop a savegroup. • Query the media database and client file indexes.
Monitor NetWorker	The ability to: • Monitor NetWorker operations, including device status, save group status, and messages. • View media databases information. • View NetWorker configuration information (except the security settings described in the Change Security Settings privilege).
Operate devices and jukeboxes	The ability to perform device and autochanger operations, for example, mounting, unmounting, and labeling. Users with this privilege can also view device status and pending messages, as well as view information in the media database.
Recover local data	The ability to recover data from the NetWorker server to their local client, as well as view most attributes in the client's configuration. Members can also query the client's save sets and browse its client file index. This privilege does not provide permission to view information about other clients and does not override file-based privileges. Users can only recover files with the appropriate user privileges for that operating system.
Backup local data	The ability to: • Manually back up data from their local client to the NetWorker server. • View most attributes in the client's configuration. • Query the client save sets and browse the client file index. This privilege does not provide permission to view information about other clients and does not override file-based privileges. Users can only back up files with the appropriate user privileges for that operating system.

NetWorker Privilege	Allowed Operations
View application settings	The ability to view NetWorker resources including: Archive Requests, Client resources, Device resources, Directives, Group, Jukebox, Label, License, Notification, Policies, Pool, Schedule, Staging, and Storage Node. It also allows user group members to view the status of operations. This privilege does not allow user group members to view the Server, user groups, or Security Audit Log resources.
Change application settings	The ability to change NetWorker resources including: Archive Requests, Client resources, Device resources, Directives, Group, Jukebox, Label, License, Notification, Policies, Pool, Schedule, Staging, and Storage Node. It also allows user group members to view the status of operations. This privilege does not allow user group members to change the Server, user groups, or Security Audit Log resources.
Create application settings	The ability to create NetWorker resources including: Archive Requests, Client resources, Device resources, Directives, Group, Jukebox, Label, License, Notification, Policies, Pool, Schedule, Staging, and Storage Node. It also allows user group members to view the status of operations. This privilege does not allow user group members to change the Server, user groups, or Security Audit Log resources.
Delete application settings	The ability to delete NetWorker resources including: Archive Requests, Client resources, Device resources, Directives, Group, Jukebox, Label, License, Notification, Policies, Pool, Schedule, Staging, and Storage Node. It also allows user group members to view the status of operations. This privilege does not allow user group members to delete the Server, or User Groups resources.
Archive data	The ability to archive data. The NetWorker application administrator must have configured NetWorker for a user with this privilege to execute this operation. Only the Client resource that pertains to the client that issues the archive command is viewable.
Backup remote data	Allows users to remotely backup data.
Recover remote data	Allows users to recover remotely backed up data.

The NetWorker Verify feature is used to provide integrity of stored backup data by ensuring that backup data on the NetWorker server matches the data on the local disk. This feature compares the file types, file modification times, file sizes, and file contents, but excludes other system or file attributes, such as access control lists, file attributes, etc. NetWorker alerts operators to any changes that have occurred to data since the backup. Verification also determines whether a hardware failure prevented the NetWorker server from completing a successful backup. It also provides a way to test the ability to recover backup data.

To protect the confidentiality of backup data in transit and on tape/disk, the NetWorker client performs AES-256 encryption on backup and archive data. The NetWorker client encrypts the data sent to the storage node, where it is transferred to a storage device. The backup data remains encrypted until a restore is requested. The encrypted backups are protected with the Datazone Encryption Key, which is encrypted with a key generated by PBKDF2 using a user-defined Datazone Pass-Phrase.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_ITT.1, FDP_ROL.2, FDP_SDI.1.

7.1.4 Identification and Authentication

Identification and authentication functions deal with how a user's identity is asserted and subsequently verified by the TOE. NetWorker supports external authentication, which allows the TOE to be integrated with an existing LDAPv1.3 compliant directory, such as OpenLDAP, or Active Directory. When a user accesses the TOE, the TOE leverages the CST to pass user credentials to a remote LDAP server for verification. During authentication, password character feedback is obfuscated. Upon successful validation of the user's credentials, a token is created, which is used to authenticate the user and determine the user's authorization. After three unsuccessful authentication attempts, the TOE presents a warning message to the user; upon acknowledgement of the warning message, the NMC application is terminated.

Subjects, or user sessions, are bound to the security role for which an association has been established with an external LDAP group. If a user is not a member of any of the associated external groups, the TOE denies access to the user. Any changes to the external role membership, or changes to the association of external roles with local security roles, require a user to re-authenticate for the changes to take effect.

Users accessing the NetWorker User interface and NetWorker CLIs are not required to authenticate prior to performing backup and recovery operations. Rather, identification and authentication is performed via the underlying OS login facility. Authorization checks ensure that the identified user possesses the required privileges before allowing any actions to be performed.

TOE Security Functional Requirements Satisfied: FIA_AFL.1, FIA_UAU.1, FIA_UAU.7, FIA_UID.2

7.1.5 Security Management

Security Management functions define how the security functionality of the TOE is managed, the roles that are authorized to perform management functions, and the management of attributes that dictate the security functionality.

The NMC is the primary management interface for the TOE. It provides several functions for managing NetWorker resources, including NMC authentication, NetWorker server and client management, storage node, device, and media management, audit logs, backup and recovery operations, save sets, policies, schedules, etc., as well as reporting and monitoring of the overall NetWorker deployment.

The NMC roles are detailed in Table 18 below, as well as the privileges associated with each role.

Table 18 NMC Roles

Role	Privileges

Console Security Administrator	• Add, delete, and modify NMC Users.
	• Configure login authentication such as configuring the NMC server to:
	  ○ use LDAP authentication instead of native NMC authentication.
	  ○ use native NMC authentication instead of LDAP authentication.
	• Control user access to managed applications such as a NetWorker server.
	• All tasks available to a 'Console User' role.

Role	Privileges
Console Application Administrator	• Configure NMC system options. • Set retention policies for reports. • View custom reports. • Specify the NetWorker server to backup the NMC database. • Specify a NetWorker License Manager server. • Run the Console Configuration wizard. • All tasks available to a Console User role.
Console User	All tasks except for those tasks explicitly mentioned for the Console Security Administrator and the Console Application Administrator. Tasks include: • Add/delete hosts, folders. • Add/Delete Managed applications for NetWorker, Data Domain, and Avamar. • Create/Delete their reports. • Set features for managed applications. • Manage a NetWorker server with the appropriate privilege levels. • Dismiss events.

In addition, each NetWorker server maintains authorization for client users based on user groups. The user groups and their associated privileges are defined in Table 19 below.

Table 19 NetWorker Server User Groups

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 • Operate NetWorker • Monitor NetWorker • Operate Devices and Jukeboxes • Recover Local Data • Recover Remote Data • Backup Local Data • Backup Remote Data • Create Application Settings • View Application Settings • Change Application Settings • Delete Application Settings • Archive Data
Monitors	• Monitor NetWorker • Operate Devices and Jukeboxes • Recover Local Data • Recover Remote Data • Backup Local Data • Backup Remote Data • View Application Settings • View Security Settings • Archive Data

User Group	Privileges
Operators	• Remote Access All Clients • View Application Settings • Operate NetWorker • Monitor NetWorker • Operate Devices and Jukeboxes • Recover Local Data • Recover Remote Data • Backup Local Data • Backup Remote Data • Archive Data
Auditors	• View security settings
Users	• Monitor NetWorker • Recover Local Data • Backup Local Data
Database Operators	• Remote Access All Clients • Operate NetWorker • Monitor NetWorker • Operate Devices and Jukeboxes • Recover Local Data • Recover Remote Data • Backup Local Data • Backup Remote Data • Archive Data
Database Administrators	• Remote Access All Clients • Configure NetWorker • Operate NetWorker • Monitor NetWorker • Operate Devices and Jukeboxes • Recover Local Data • Recover Remote Data • Backup Local Data • Backup Remote Data • Archive Data

Security attributes for TSF management functions, particularly those available to a Console Security Administrator or Security Administrator, are provided with secure default values. For example, new Console users are given Console User role privileges. When managing NetWorker server resources, new User Groups contain no privileges by default. Only the Console Security Administrator or Security Administrator may provide alternative values upon the creation of a resource. In addition, NMC Roles do not automatically grant a user NetWorker server privileges, and vice versa. In order to access a NetWorker server managed through the NMC, the user must also be assigned the appropriate NetWorker server privileges via User Group membership.

TOE Security Functional Requirements Satisfied: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1.

7.1.6 Protection of the TSF

The TOE is capable of recovering from several types of disaster scenarios, including hardware failures, loss of network connectivity, and primary storage software failures. The NetWorker server backs up the

NetWorker server and NMC server database on a regular schedule, allowing for the TOE to be restored to a secure state.

Additionally, in the event client software/hardware failure, or loss of network connectivity during a backup operation, the Checkpoint Restart feature is used to recover from a point of failure without the need to resave the entire save set. Normally, if the backup operation is interrupted, or a crash occurs, the save set is discarded or is marked as incomplete and recyclable. CheckPoint Restart allows a failed backup operation to restart at a known good point, prior to the point of failure. CheckPoint Restart creates a sequence of linked partial save sets if the save operation is interrupted. A save can be restarted and continue saving file system data from the point of failure. Each subsequent restart will produce a new save set in a checkpoint restart sequence.

Checkpoint Restart offers two operating modes:

- **checkpoint by file** — A checkpoint is created after saving each file system entry (file, directory, and link).
- **checkpoint by directory** — A checkpoint is created each time a directory is saved. If a large number of directory entries are present, intermediate checkpoints are created automatically between directories.

Communications between NetWorker daemons are secured using *libcommonSSL* along with the underlying cryptographic support from the BSAFE Crypto-C ME library. All TSF data is transferred through a mutually authenticated TLS session.

TOE Security Functional Requirements Satisfied: FPT_FLS.1, FPT_ITT.1.

7.1.7 Resource Utilization

The TOE provides limited fault tolerance in the event of a failed backup operation; CheckPoint Restart backups allow a failed save operation to continue from the point of failure. Client backups are directed to the storage nodes, therefore, in the event of a NetWorker server failure, clients continue to send backup data, however no new operations can take place until the NetWorker server is restored.

NetWorker software monitors the storage node to ensure that the storage node is still functioning. The *nsrmon* process communicates with *nsrexecd* on the storage node to get the *nsrmmd* status. Based on the node status, the server might take some set of actions. For example, the server might attempt to start a storage node process, if it expected one to be running. If the polling event times out, the server assumes that the storage node is not functional. This type of polling is necessary in order to allow the node failover function to work properly. The failover function occurs when a client's savestream is directed to the next functional storage node as determined by its storage nodes attribute.

Additionally, NetWorker operators may designate, in order of priority, the storage node that a client's data should be directed to. If the first storage node listed for the client is not available, the next storage node on the list is contacted to receive the backup data.

NetWorker also defines minimum retention lock periods for the protection of stored user data from modification and deletion. This is enforced through NetWorker browse and retention policies. A browse policy determines how long files are maintained in a client's index on the NetWorker server. During this period, users can browse backed-up data from the NetWorker client computer, and select individual files or entire file systems for recovery. After the browse policy time period has expired, the entry for that file is deleted from the NetWorker server. A retention policy specifies the period of time which backed-up data is protected from accidental overwrite. After the retention period is exceeded, the save set is eligible to change its status from recoverable to recyclable. The term recyclable means "eligible for recycling." The save set's status, however, does not change to recyclable until it, and all the save sets that depend on it, have passed their retention policy. The NetWorker server keeps track of save set dependencies regardless

of whether the dependent save sets are stored on the same or different volumes. The expiration of a save set's retention policy does not remove the save set's entries from the media database.

TOE Security Functional Requirements Satisfied: FRU_FLT.1, EXT_FRU_DRP.1.

7.1.8 TOE Access

The NMC client displays a login banner, which is a localized string value added to the login dialog prior to identification and authentication. The default text is "Warning: Authorized user only"; however the banner text is configurable by the Console Application Administrator.

TOE Security Functional Requirements Satisfied: FTA_TAB.1.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3.

8.2 Security Objectives Rationale

This section provides a rationale for the existence of each threat, policy statement, and assumption that compose the Security Target. Sections 8.2.1, 8.2.2, and 8.2.3 demonstrate the mappings between the threats, policies, and assumptions to the security objectives are complete. The following discussion provides detailed evidence of coverage for each threat, policy, and assumption.

8.2.1 Security Objectives Rationale Relating to Threats

Table 20 below provides a mapping of the objects to the threats they counter.

Table 20 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.COMPROMISE Critical system or user data may be compromised due to a failure, rendering data unusable. Threat agent is an environmental condition or force that results in hardware failure.	O.BACKUP The TOE must protect user data by implementing a backup and recovery mechanism that ensures integrity, availability, and confidentiality of backup data.	O.BACKUP provides assurance that critical system and user data is backed up according to a schedule, and may be restored to a previous state if data compromise occurs.
T.DATALOSS Backups of critical system or user data may be overwritten, modified, or accessed by an unauthorized user.	O.BACKUP The TOE must protect user data by implementing a backup and recovery mechanism that ensures integrity, availability, and confidentiality of backup data.	O.BACKUP provides assurance that backup sets are prevented from becoming overwritten using media retention policies. It also prevents unauthorized modification by verifying the integrity of backup data. To prevent unauthorized access, data written to backup media is encrypted by the TOE.
T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	By ensuring that The TOE is able to identify and authenticate users prior to allowing access to TOE administrative functions and data, O.AUTHENTICATE satisfies this threat.
T.TAMPERING A user or process may be able to bypass the TOE's security mechanisms by tampering with the TOE or TOE environment.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.

Threats	Objectives	Rationale
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that security relevant events that may indicate attempts to tamper with the TOE are recorded.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.
	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT ensures that the TOE is protected from external interference or tampering.
T.UNAUTH A user may gain access to security data on the TOE, even though the user is not authorized in accordance with the TOE security policy.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	The objective O.ADMIN ensures that access to TOE security data is limited to those users with access to the management functions of the TOE.
	O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.	The objective O.AUDIT ensures that unauthorized attempts to access the TOE are recorded.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	The objective O.AUTHENTICATE ensures that users are identified and authenticated prior to gaining access to TOE security data.

Threats	Objectives	Rationale
T.WEAKCRYPTO An unauthorized user may exploit a weakness in a protocol or algorithm to gain access to sensitive information handled by the TOE.	O.CRYPTO The TOE must incorporate a FIPS 140-2 validated module that provides approved functions for key generation, destruction, and cryptographic operations.	O.CRYPTO provides assurance that the cryptography implemented by the TOE to protect system and user data has been FIPS validated.

Every Threat is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives counter all defined threats.

8.2.2 Security Objectives Rationale Relating to Policies

Table 21 below gives a mapping of policies and the objectives that support them.

Table 21 Policies: Objectives Mapping

Policies	Objectives	Rationale
P.MANAGE The TOE may only be managed by authorized users.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN ensures that the TOE provides the necessary tools to support the P.MANAGE policy.
	O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	O.AUTHENTICATE ensures that only authorized users are granted access to the tools required to manage the TOE.
P.INTEGRITY Data collected and produced by the TOE must be protected from modification.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	O.ADMIN ensures that the TOE provides the necessary tools to support the P.INTEGRITY policy.
	O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	O.PROTECT ensures that the TOE protects audit and system data to meet this policy.

Every policy is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives enforce all defined policies.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 22 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 22 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.INSTALL The TOE is installed on the appropriate, dedicated hardware and operating system.	OE.PLATFORM The TOE hardware and OS must support all required TOE functions.	OE.PLATFORM ensures that the TOE hardware and OS supports the TOE functions.
	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	Those responsible for the TOE will provide competent individuals to perform management of the security of the environment, and restrict these functions and facilities from unauthorized use. OE.MANAGE satisfies this assumption.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF.
A.LOCATE The TOE, and all TSF-dependent services, including the LDAP server used for authentication and authorization, are located within a secure, controlled access facility.	OE.PHYSICAL The physical environment must be suitable for supporting a computing device in a secure setting.	Physical security is provided within the TOE environment to provide appropriate protection to the network resources. OE.PHYSICAL satisfies this assumption.
A.NOEVIL The users who manage the TOE, and the TSF-dependent services in the IT Environment, are non-hostile, appropriately trained, and follow all guidance.	OE.MANAGE Sites deploying the TOE will provide competent, non-hostile TOE administrators who are appropriately trained and follow all administrator guidance. TOE administrators will ensure the system is used securely.	OE.MANAGE satisfies the assumption that the users who manage the TOE are non-hostile, appropriately trained and follow all guidance.
A.PROTECT The TOE software will be protected from unauthorized modification.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	The TOE environment provides protection from external interference or tampering. OE.PROTECT satisfies this assumption.
A.TIMESTAMP The IT environment provides the TOE with the necessary reliable timestamps.	OE.TIME The TOE environment must provide reliable timestamps to the TOE.	OE.TIME satisfies the assumption that the environment provides reliable timestamps to the TOE.

Every assumption is mapped to one or more Objectives in the table above. This complete mapping demonstrates that the defined security objectives uphold all defined assumptions.

8.3 Rationale for Extended Security Functional Requirements

An extended SFR called EXT_FRU_DRP.1: Minimum retention lock periods was created to address the retention lock functionality of the TOE. The FRU_RSA.1 SFR (Maximum quotas) was used as a model for creating this SFR. This requirement has no dependencies since the stated requirement embodies all of the necessary functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus does not require any additional Assurance Documentation.

8.4 Rationale for Extended TOE Security Assurance Requirements

No Extended SARs are defined in this ST.

8.5 Security Requirements Rationale

The following discussion provides detailed evidence of coverage for each security objective.

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 23 below shows a mapping of the objectives and the SFRs that support them.

Table 23 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must include a set of functions that allow efficient management of its functions and data, ensuring that TOE users with the appropriate privileges and only those TOE users, may exercise such control.	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts access to security attribute data based on the user's role.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that security attributes are given restrictive or permissive values where necessary, and that only authorized users may provide alternative default values.

Objective	Requirements Addressing the Objective	Rationale
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by ensuring that the TOE includes administrative functions to facilitate the management of the TSF.
	FMT_SMR.1 Security roles	The requirement meets the objective by ensuring that the TOE associates users with roles to provide access to TSF management functions and data.
O.AUDIT The TOE must record events of security relevance at the "not specified level" of audit. The TOE must record the resulting actions of the security functional policies, prevent unauthorized modification of the audit trail, prevent loss of audit trail data, and provide the authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets this objective by ensuring that the TOE associates each auditable event with the identity of the user that caused the event.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.3 Action in case of possible data loss	If the audit facilities become full, the TOE ensures that new log files are created once a size limit is reached. This requirement meets this objective by mitigating the risk of loss of audit trail data.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_AFL.1 Authentication failure handling	The requirement meets the objective by ensuring that brute force attacks against the TOE are thwarted using authentication failure thresholds, which terminate the process performing authentication after a pre-defined amount of failures.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that users are authenticated before access to TSF-mediated functions is allowed.

Objective	Requirements Addressing the Objective	Rationale
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UAU.7 Protected authentication feedback	The process that identifies and authenticates users ensures that authentication data is obscured during entry.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the users are identified before access to TOE administrative functions is allowed.
O.AUTHENTICATE The TOE must be able to identify and authenticate users prior to allowing access to TOE administrative functions and data.	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE authenticates users prior to allowing access to administrative functions to ensure that only those trusted users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that only authorized users are allowed access to security attributes.
O.BACKUP The TOE must protect user data by implementing a backup and recovery mechanism that ensures integrity, availability, and confidentiality of backup data.	FDP_ITT.1 Basic internal transfer protection	The requirement meets the objective by ensuring that backup data is protected from disclosure while in transit.
	FDP_ROL.2 Advanced rollback	The requirement meets the objective by ensuring that user data is available to be recovered to a previous trusted state, and may only be restored by authorized users to authorized devices.
	FDP_SDI.1 Stored data integrity monitoring	The requirement meets the objective by ensuring that recovered data is free of integrity errors.
	EXT_FRU_DRP.1 Minimum retention lock periods	The requirement meets the objective by ensuring that the TOE ensures availability of offline backups by instating data retention policies on backup sets.
O.CRYPTO The TOE must incorporate a FIPS 140-2 validated module that provides approved functions for key generation, destruction, and	FCS_CKM.1 Cryptographic key generation	The requirement meets the objective by ensuring that all cryptographic keys are generated using an approved random number generator.

Objective	Requirements Addressing the Objective	Rationale
cryptographic operations.	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that all cryptographic keys are destroyed using an approved zeroization technique.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that all encryption/decryption, hashing, and signing operations are performed using approved cryptographic algorithms.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its functions and data.	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that no one may delete or alter information in the audit logs.
	FAU_STG.3 Action in case of possible data loss	The requirement meets the objective by ensuring that audit logs are prevented from exceeding a certain size limit.
	FDP_ACC.1 Subset access control	The requirement meets the objective by ensuring that access control is applied to all actions requested by a user.
	FDP_ACF.1 Security attribute based access control	The requirement meets the objective by ensuring that the TOE protects itself by enforcing a lockout after a configurable number of unsuccessful authentication attempts.
	FIA_AFL.1 Authentication failure handling	In order to ensure that users are properly authenticated prior to access, the TOE terminates the authentication process after a pre-defined number of unsuccessful authentication attempts. The requirement for TOE session establishment meets the objective by mitigating the risk of a brute force attack on a username and password.
	FIA_UAU.1 Timing of authentication	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authenticated users are allowed access to TSF-mediated functions.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only identified users are allowed access to TOE functions.
	FMT_MOF.1 Management of security functions behaviour	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only privileged users may manage the security behaviour of the TOE.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the TOE protects itself from unauthorized modification. The TOE does this by ensuring that only authorized users have access to manage security attributes.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that security attributes are given secure default values when an object is created.
	FRU_FLT.1 Degraded fault tolerance	The requirement meets the objective by ensuring that the TOE provides mechanisms for ensuring the security of backup data given a degraded state.
	FPT_ITT.1 Basic internal TSF data transfer protection	The requirement meets the objective by ensuring that TSF data is transmitted between separate parts of the TOE through a mutually authenticated session.
O.PROTECT The TOE must ensure the integrity of audit and system data by protecting itself from unauthorized modifications and access to its	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that the TOE is capable of returning to a secure state if a failure condition occurs.

Objective	Requirements Addressing the Objective	Rationale
functions and data.	FTA_TAB.1 Default TOE access banners	The requirement meets the objective by ensuring that unauthenticated users are given an advisory notice regarding unauthorized use of the TOE prior to identification and authentication.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. While the System may monitor a hostile environment, it is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2, the System will have incurred a search for obvious flaws to support its introduction into the non-hostile environment. The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 24 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 24 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	No	The OS is part of the TOE environment, thus accurate timestamps are provided by the TOE environment. This dependency is met instead by OE.TIME.
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.3	FAU_STG.1	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FCS_CKM.1	FCS_COP.1	✓	
	FCS_CKM.4	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.1	✓	
	FCS_CKM.4	✓	
FDP_ACC.1	FDP_ACF.1	✓	
FDP_ACF.1	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_ITT.1	FDP_ACC.1	✓	
FDP_SDI.1	No dependencies	✓	
FIA_AFL.1	FIA_UAU.1	✓	
FIA_UAU.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FIA_UAU.7	FIA_UAU.1	✓	
FIA_UID.2	No dependencies	✓	
FMT_MOF.1	FMT_SMR.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.1	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
	FDP_IFC.1	✓	
	FMT_SMF.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	✓	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not included, FIA_UID.2, which is hierarchical to FIA_UID.1 is included. This satisfies this dependency.
FRU_FLT.1	FPT_FLS.1	✓	
EXT_FRU_DRP.1	No dependencies	✓	
FPT_ITT.1	No dependencies	✓	

SFR ID	Dependencies	Dependency Met	Rationale
FPT_FLS.1	No dependencies	✓	
FTA_TAB.1	No dependencies	✓	

9 Acronyms and Terms

This section defines the acronyms and terms used throughout this document.

9.1 Acronyms

Table 25 Acronyms and Terms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Counter with CBC-Message Authentication Code (MAC)
CEM	Common Evaluation Methodology
CFB	Cipher Feedback
CM	Configuration Management
CPU	Central Processing Unit
CST	Common Security Toolkit
CTR	Counter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
EC	Elliptic Curve
ECB	Electronic Codebook
FIPS	Federal Information Processing Standard
GCM	Galois Counter Mode
GB	Gigabyte
GMAC	Galois Message Authentication Code
GPC	General Purpose Computer
GST	Generic Services Toolkit
GUI	Graphical User Interface
HMAC	Hash-Based Message Authentication Code
HP	Hewlett Packard

Acronym	Definition
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
ID	Identifier
IT	Information Technology
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MB	Megabyte
ME	Micro Edition
NAS	Network Attached Storage
NDMP	Network Data Management Protocol
NIST	National Institute of Standards and Technology
NMC	NetWorker Management Console
OFB	Output Feedback
OS	Operating System
OSP	Organizational Security Policy
PBKDF	Password-Based Key Derivation Function
PKCS	Public Key Cryptography Standard
PP	Protection Profile
PRNG	Pseudo-Random Number Generator
PSS	Probabilistic Signature Scheme
RAM	Random Access Memory
RPC	Remote Procedure Call
RSA	Rivest, Shamir, Adleman
RSASSA	RSA Signature Scheme with Appendix
SAR	Security Assurance Requirement
SAP	System Analysis and Program Development AG
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol

Acronym	Definition
SP	Special Publication
SQL	Structured Query Language
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VCB	VMware Consolidated Backup

9.2 Terminology

NetWorker client – The NetWorker client software communicates with the NetWorker server and provides client initiated backup and recovery functionality. The NetWorker client software is installed on all machines that are backed up to the NetWorker server.

NetWorker storage node – Data is backed up directly to devices local to a NetWorker server or remotely to a NetWorker storage node. A storage node controls storage devices such as tape drives, disk devices, autochangers, and silos. The NetWorker server is a local storage node.

NetWorker server – The NetWorker server provides services to back up and recover data for the NetWorker client machines in a datazone. The NetWorker server can also act as a storage node and control multiple remote storage nodes.

NetWorker Management Console (NMC) server – The NMC server, or Console server, is a Java based web application server that provides centralized management, monitoring, and reporting of multiple NetWorker servers across multiple datazones.

NetWorker datazone – A NetWorker datazone is a single NetWorker server and its client and storage node machines.

Prepared by:
Corsec Security, Inc.

13135 Lee Jackson Memorial Highway
Suite 220
Fairfax, VA 22033
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com