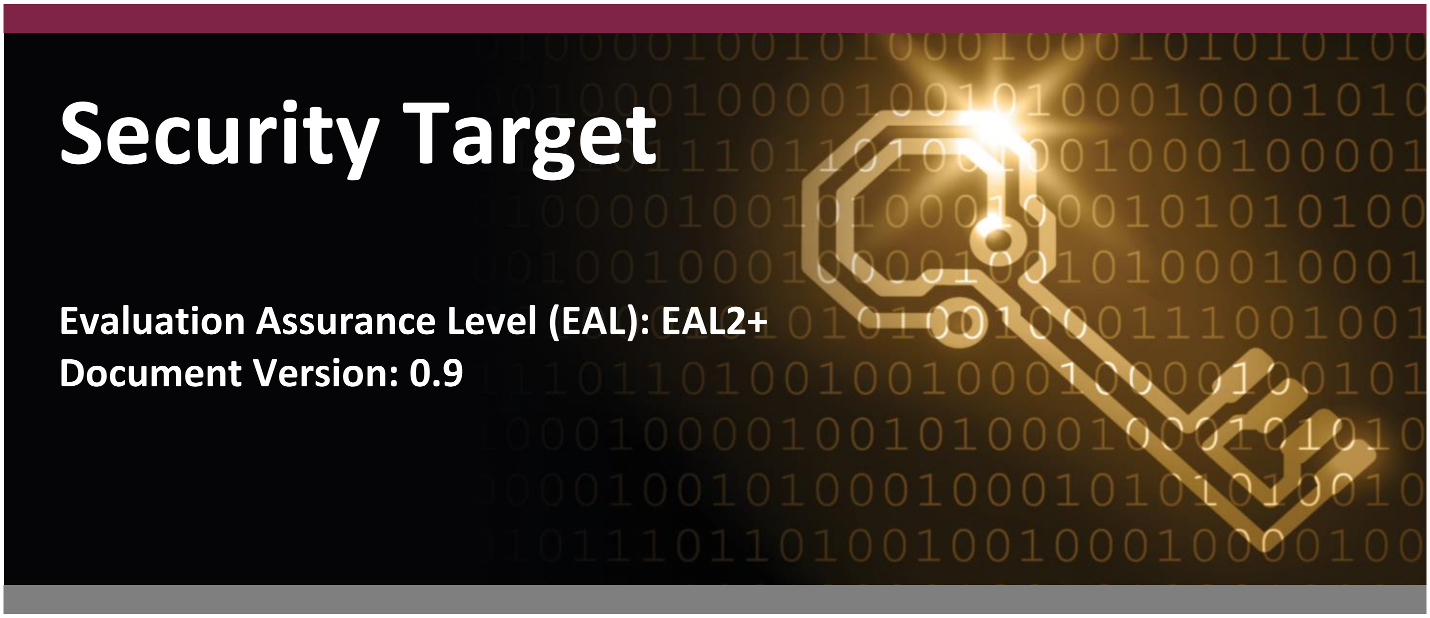
Nimble Storage, Inc.

NimbleOS

v4.2



Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.9

Prepared for:	**Prepared by:**
Nimble Storage, Inc. 211 River Oaks Parkway San Jose, CA 95134 United States of America	**Corsec Security, Inc.** 13921 Park Center Road, Suite 460 Herndon, VA 20171 United States of America
Phone: +1 408 432 9600 www.nimblestorage.com	Phone: +1 703 267 6050 www.corsec.com

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is Nimble Storage, Inc. NimbleOS v4.2.0.1-499435-opt and will hereafter be referred to as NimbleOS v4.2 or the TOE throughout this document. The TOE is an operating system (OS) running on Nimble arrays that provides data protection and storage management for the storage system. The TOE provides secure access to storage on the Nimble arrays for both iSCSI[1] and Fibre Channel (FC) clients. The TOE also provides a Web-based graphical user interface (GUI) built upon a REST[2] API[3] and a command-line interface (CLI) for administration.

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 SFRs 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] iSCSI – Internet Small Computer System Interface

[2] REST – Representational State Transfer

[3] API – Application Programming Interface

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	Nimble Storage, Inc. NimbleOS Security Target
ST Version	Version 0.9
ST Author	Corsec Security, Inc.
ST Publication Date	11/8/2017
TOE Reference	Nimble Storage, Inc. NimbleOS v4.2.0.1-499435-opt
FIPS[4] 140-2 Status	Level 1 Validated Cryptographic Module: Nimble Storage, Inc. FIPS Object Module cert# 2422

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

1.3.1 NimbleOS Overview

NimbleOS is a predictive flash storage solution that can be deployed on Nimble's all-flash or hybrid flash arrays. NimbleOS protects data while providing unparalleled efficiency in a SAN[5] array. The array can be accessed over iSCSI or FC. Data protection is offered with triple+ parity RAID[6] 6 and optional data at rest encryption. NimbleOS supports scheduled and manual volume snapshots and application synchronization as well as data replications across the cluster. Data is compressed and de-duplicated inline.

NimbleOS provides adaptive flash service levels for different applications with All Flash, Auto Flash, or Minimal Flash settings that allow SAN administrators to determine the best operation for their environment and change these configurations on the fly. This allows NimbleOS to adapt rapidly to application workload changes and support simultaneous diverse workloads without contention among resources in the array. All Flash makes more efficient use of the flash resources using Nimble's patented Cache Accelerated Sequential Layout (CASL™) architecture and pinning data in cache. Auto Flash balances high performance and capacity. Minimal Flash uses disk-only services to optimize capacity.

Up to four arrays can be combined into a scale-out cluster (or group) logically representing a single storage entity. The cluster is primarily administered through a management IP[7] address hosted on one of the arrays in the group. As illustrated in Figure 1, subsets of the arrays within a group can be confined to disjoint pools. Volumes may reside in a single array in a pool or cross multiple arrays in the same pool. Data is automatically rebalanced across the pool. When configuring groups, an array is designated as the Group Leader (GL), and a different array is the Backup Group Leader (BGL). The GL monitors the arrays within the group and sends group policies to all arrays within the group.

[4] FIPS – Federal Information Processing Standard
[5] SAN – Storage Area Network
[6] RAID – Redundant Array of Independent Disks
[7] IP – Internet Protocol

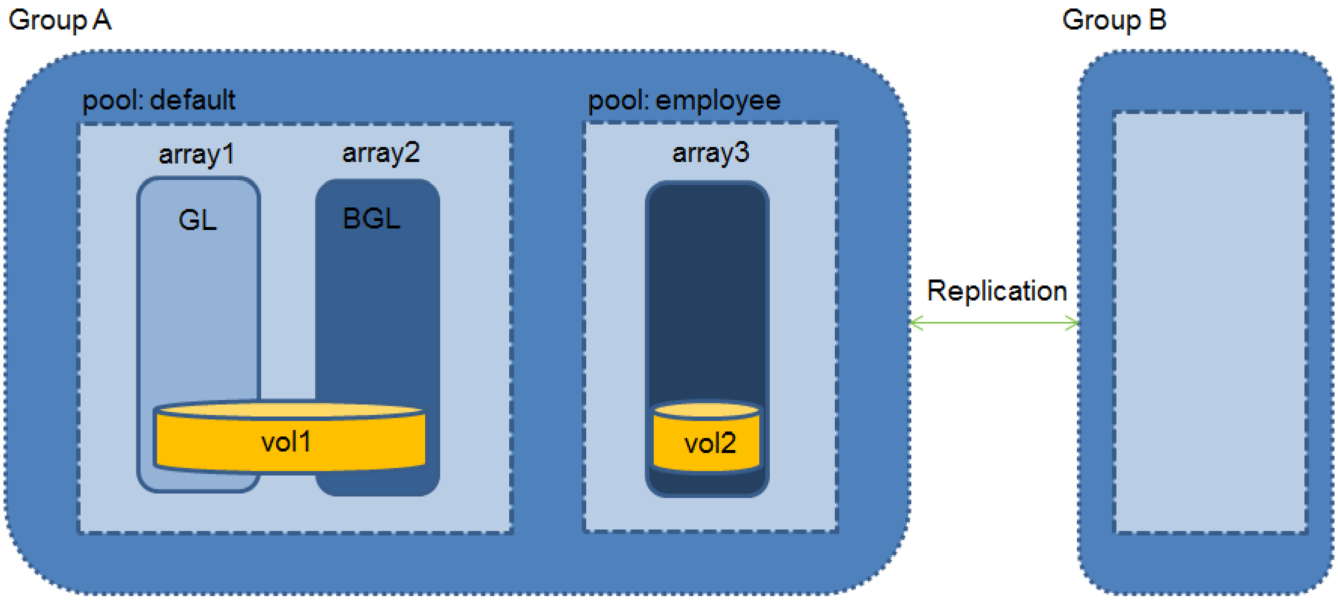


Figure 1 – Depiction of Groups, Pools, and Arrays within NimbleOS

Data protection is provided by snapshots that are stored on the same array as production data, allowing instant data restore and WAN[8]-efficient replication. NimbleOS's thin, point-in-time snapshots of a volume's metadata[9] allow frequent snapshots to be stored on a single array and volumes to be rolled back to a desired point-in-time using a very small amount of resources and storage space. Snapshots can even create fully functioning clones of volumes. NimbleOS also supports remote replication of individual volumes for disaster recovery. Replication can take place from array to array or from group to group. When replicating, only compressed, changed data blocks are sent over the network, minimizing network impact.

The Nimble Storage SmartSecure software-based encryption provides data at rest encryption for NimbleOS. It uses the AES[10] XTS[11] with 256-bit keys on block oriented storage devices and leverages the AES-NI[12] instruction set on the underlying hardware. Encryption can be configured per volume or array group. Once data is encrypted, it remains encrypted when transferred between arrays.

NimbleOS provides failover capability by instantly mirroring data from an active to standby controller NVRAM[13]. The standby controller is in an online ready state with a bit-for-bit memory image to sustain controller failover instantly with no outage or downtime. In addition, NimbleOS leverages its triple+ parity RAID to protect against up to three (on all-flash arrays) or two (on hybrid flash arrays) simultaneous drive failures without loss of data. This same RAID feature protects against partial data loss by allowing an array to recover from bit errors discovered through continuous data integrity monitoring.

NimbleOS supports non-disruptive scaling to fit changing application needs through increased performance, capacity, or both. Administrators can non-disruptively upgrade controllers or swap in additional disk shelves or

[8] WAN – Wide Area Network
[9] Metadata is information about the data itself, e.g., where a block of data is stored on the SSD.
[10] AES – Advanced Encryption Standard
[11] XTS – XEX(Exclusive Or (XOR) Encrypt XOR) Tweakable block cipher with ciphertext Stealing
[12] NI – New Instruction
[13] NVRAM - Non-volatile random-access memory

solid state drives (SSDs). They can also perform non-disruptive software upgrades, maximizing uptime and user productivity through continuous availability.

NimbleOS is delivered installed on an array that occupies a 4U[14] rack unit. Currently, the following models of arrays are supported:

- Adaptive Flash Arrays:
  - CS1000 and CS1000H support small to medium-sized organizations.
  - CS3000 supports medium IT[15] organizations or distributed sites of larger organizations.
  - CS5000 supports larger-scale deployments.
  - CS7000 is designed for consolidating multiple large-scale critical applications with aggressive storage demands.
- All Flash Arrays:
  - AF1000 and AF3000 are entry level all flash arrays for IT organizations that require speed and economy for performance-sensitive workloads.
  - AF5000 and AF7000 deliver high performance and attractive economics for performance-sensitive workloads that require the best blend of price/performance/scalability.
  - AF9000 is used to consolidate multiple large-scale performance-sensitive applications with aggressive performance and high scalability demands.

NimbleOS provides three management interfaces to administer the Nimble arrays:

- NimbleOS CLI – a limited OS shell
- NimbleOS GUI – a Web-based GUI
- NimbleOS API – a REST API

Figure 2 (below) depicts a typical Nimble Storage, Inc. array.

Figure 2 – Nimble Storage Array

[14] U – Unit

[15] IT – Information Technology

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type and describing the TOE.

The TOE is an OS running on Nimble Storage arrays that provides data protection and storage and backup management. It implements several key security features:

- *Access control* – Storage is provisioned by way of volumes accessed over a storage network via either iSCSI or FC. The iSCSI clients, or initiators, with the proper CHAP[16] account credentials can access associated volumes. Volumes may also be accessed by both iSCSI and FC clients alike with the use of initiator groups. In this case, CHAP credentials are not required, as access is dictated by authorized user mappings between IQNs[17]/WWPNs[18] and volumes.
- *Management with RBAC[19] via the NimbleOS GUI, CLI, or API* – Authorized TOE administrators are restricted to security functions and TSF[20] data based on their role(s) assigned through a user account. There are four roles: Administrator, Power User, Operator, and Guest.
- *Multiple authentication mechanisms* – Both local and AD[21] authentication can be configured to identify and authenticate TOE administrators at the NimbleOS GUI, CLI, or API.
- *Data protection and fault tolerance* – NimbleOS protects against user data errors with checksums and continuous data integrity monitoring. It protects against hardware failures with an active/standby controller design and triple-parity RAID. It sustains failover for up to two disk failures or a single controller failure on an array.
- *Auditing* – Audit records are created for startup and shutdown and all administrator-initiated, non-read operations performed on an array. Every record identifies the administrator taking the action.
- *Snapshots* – Snapshots of volumes and volume groups can be created to preserve a point-in-time copy of one or more volume's metadata. These snapshots can be used to roll back all the operations on a volume to restore it to a desired point-in-time.
- *Export of user data* – Authorized TOE administrators can create protection schedules to export copies of volumes (or replicas) to replication partners. The copies have a checksum associated with them to ensure the data is consistent. In addition, if the volume has been encrypted, the replica that is exported remains encrypted.
- *FIPS-validated cryptographic module* – The TOE uses the Nimble Storage, Inc. FIPS Object Module to provide all cryptographic functionality. This includes encryption of data at rest on selected volumes; a protected path from remote users of the NimbleOS GUI, CLI, or API; protection of keys at rest and in transit; a trusted channel to replication partners for transfer of wrapping keys; and X.509 certificate management. TLS[22]v1.2, HTTPS[23], and SSH[24] are supported.

[16] CHAP – Challenge-Handshake Authentication Protocol
[17] IQN – iSCSI Qualified Name
[18] WWPN – World Wide Port Name
[19] RBAC – Role Based Access Control
[20] TSF – TOE Security Functionality
[21] AD – Active Directory
[22] TLS – Transport Layer Security
[23] HTTPS – Hypertext Transfer Protocol Secure
[24] SSH – Secure Shell

1.4.1 Brief Description of the Components of the TOE

The software TOE is comprised of NimbleOS, which is a software binary that is preinstalled on the arrays shipped by Nimble. The TOE is uniquely identified as Version 4.2.0.1-499435-opt.

1.4.2 TOE Environment

The TOE is preinstalled on Nimble iSCSI and FC arrays and is intended to be deployed in a secure data center that protects physical access to the TOE.

In a typical deployment scenario, the TOE may be deployed on a group of up to four physically connected arrays of the same type (iSCSI or FC) managed as a single entity. Each array in the group is running NimbleOS v4.2 and communicating with other arrays in the same or a different group over a network. The TOE is supported on the following Nimble arrays: CS1000, CS1000H, CS3000, CS5000, CS7000, AF1000, AF3000, AF5000, AF7000, and AF9000.

The evaluated configuration consists of two groups that each consist of a single array. One group includes a CS1000 iSCSI array; the other includes an AF1000 FC array. Figure 3 below shows the details of the evaluated configuration of the TOE with the two groups indicated as Group A and Group B. The following previously undefined acronyms appear in Figure 3:

- LAN – Local Area Network
- NTP – Network Time Protocol
- R2 – Release 2

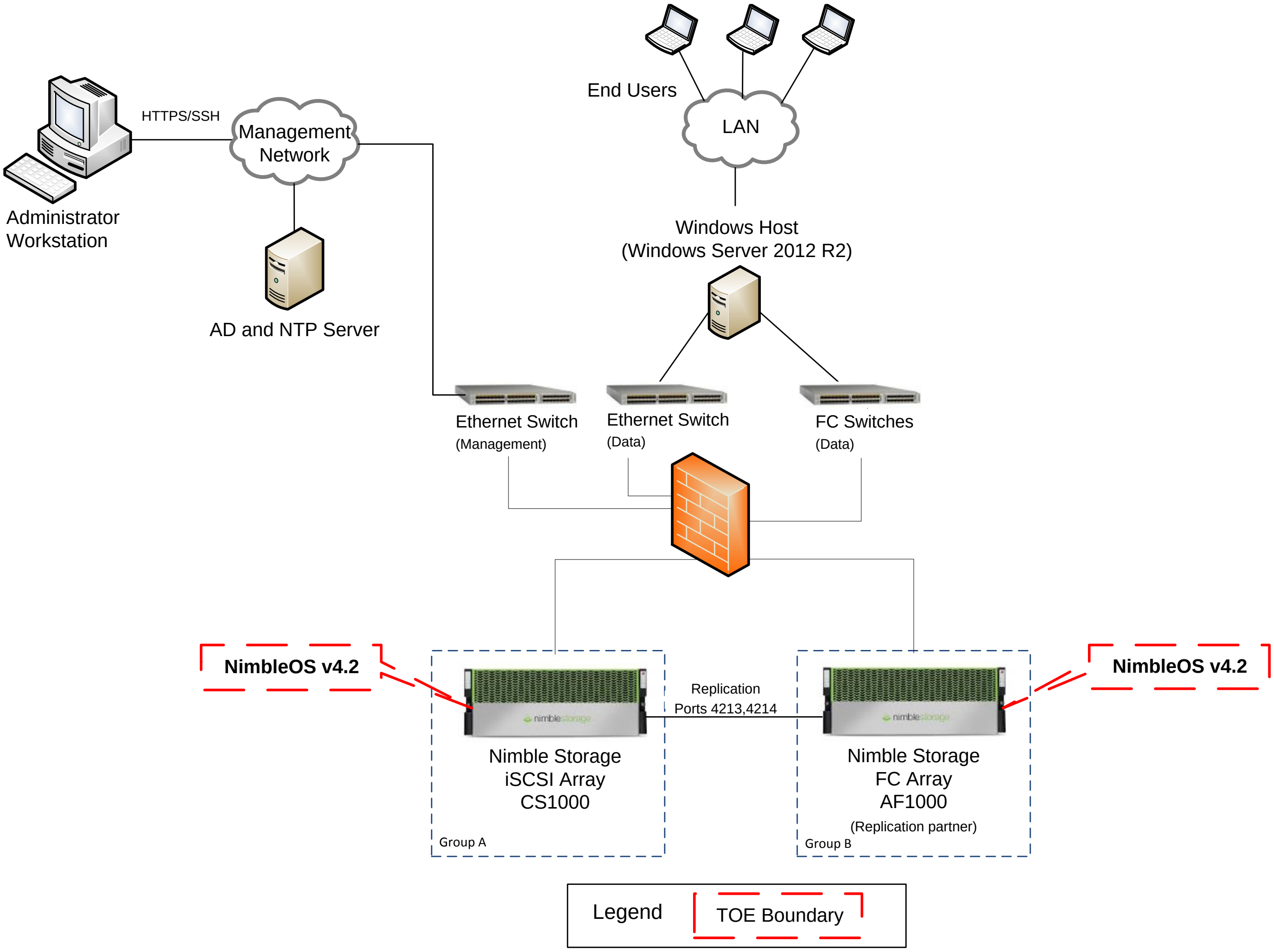

HTTPS/SSH
Management Network
Administrator Workstation
AD and NTP Server
End Users
LAN
Windows Host (Windows Server 2012 R2)
Ethernet Switch (Management)
Ethernet Switch (Data)
FC Switches (Data)
NimbleOS v4.2
NimbleOS v4.2
Replication Ports 4213,4214
Nimble Storage iSCSI Array CS1000
Group A
Nimble Storage FC Array AF1000
(Replication partner)
Group B
Legend
TOE Boundary

Figure 3 – Evaluated Configuration of the TOE

There are three networks (or subnets) in the evaluated configuration of the TOE:

- A 10 GbE[25] data network for iSCSI connections and traffic between the iSCSI and FC array and administrative access to the NimbleOS GUI, CLI, or API
- A 1 GbE management network for management of the TOE via the NimbleOS GUI, CLI, or API
- An FC data network for FC connections

In the evaluated configuration, switches are used to provide network connectivity.

The iSCSI initiators on the Windows host system shown in Figure 3 connect with the iSCSI array via a Virtual Target IP address. Then the connection is automatically redirected to an appropriate iSCSI IP address of one of the array's data ports. The FC initiators on the Windows host system connect over the FC switches to the FC array.

The CS1000 iSCSI and AF1000 FC array in the evaluated configuration are setup as replication partners and connected by a network over ports 4212 and 4213. The FC array receives replicas, or copies, of volumes from the

[25] GbE – Gigabit Ethernet

iSCSI array. In the case of a failure on the iSCSI array, these replicas can be restored as complete copies of the volumes, with all TSF and user data intact.

An AD and NTP server provide AD authentication and array time synchronization, respectively. Communications for the AD server are sent using SMBv2[26].

The iSCSI and FC clients of a Nimble storage system (represented as the Windows host system in Figure 3) typically serve application-specific functions, e.g., hypervisor, web server, database server, mail server, file server, etc. End-user systems connect to the iSCSI and FC clients, which are located in a controlled access facility along with the TOE, through well-defined protocols. For example, an end-user accessing an iSCSI client serving as a web server may access the client via a secure channel such as HTTPS. The end-users systems connect to the clients via an Ethernet LAN.

Each array is assigned a management IP address, which is used as primary access to the NimbleOS GUI, API, or CLI. The initial setup of the TOE is performed using the NimbleOS CLI via a serial or direct connection from the administrator workstation to the active controller on the array. Afterwards, the NimbleOS CLI may also be accessed via an SSH connection. Access to the NimbleOS GUI, API, or CLI can also be gained through the array's configured data IP addresses.

1.4.2.1 Non-TOE Hardware/Software

The TOE relies on non-TOE hardware/software for its essential operation. Though this hardware/software, including the Nimble arrays, is necessary for the TOE's operation, it is not part of the TOE. The following non-TOE hardware/software is required for essential operation of the TOE:

- Nimble Storage System hardware – Array (chassis, controllers, power supplies, storage), rail kit, serial cables, power cords
- Administrator workstation – used to access the NimbleOS GUI via an IE[27] 10.0+ or Google Chrome 20.0+ Web browser
- Ethernet and FC switches for connections to the management and data networks
- Network firewall – used to protect TOE interfaces
- Cables for management and data networks
- AD Server – Microsoft AD Domain Services for authentication
- NTP Server for array time synchronization
- iSCSI and FC client to connect to the array (evaluated with Windows host running Windows Server 2012 R2)
- SSH Client (e.g., putty) supporting SSHv2 for access to the NimbleOS CLI

1.4.3 Product Physical/Logical Features and Functionality not included in the TOE

The NimbleOS provides other security features that are out of the scope of the TOE. These features are not included in the TOE and will not be evaluated; therefore, there is no assurance level associated with them. The features not included in the TOE are the following:

- All SNMP[28] functionality

[26] SMBv2 – Server Message Block version 2
[27] IE – Internet Explorer
[28] SNMP – Simple Network Management Protocol

- Remote Syslog
- Nimble Storage System hardware
- InfoSight – cloud connected predictive analytics tool
- AutoSupport
- Secure tunnel – disabled by default
- Nimble Windows Toolkit

1.5 TOE Description

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

1.5.1 Physical Scope

The TOE is NimbleOS. NimbleOS v4.2 is a single binary that is pre-installed on each of the iSCSI and FC arrays (both Adaptive Flash and All Flash) shipped to a customer. The same binary is pre-installed on each array supported by the TOE. In the evaluated configuration, the TOE is installed on a CS1000 iSCSI array and an AF1000 FC array.

1.5.1.1 TOE Software

The TOE is comprised of the NimbleOS v4.2 software.

1.5.1.2 Guidance Documentation

The guides listed below are required reading and part of the TOE. This Nimble documentation (in PDF[29] format) is available to authorized users on the Nimble InfoSight Support Portal at https://infosight.nimblestorage.com/InfoSight/login.

- *Nimble Storage Hardware Guide, AF1000, AF3000, AF5000, AF7000, AF9000, AFS2,* Version 3, Revision A
- *Nimble Storage Array Quick Start Guide – Array Installation – All Flash,* Revision C, 03/20/2017
- *Nimble Storage Hardware Guide, CS1000H, CS1000, CS3000, CS5000, CS7000, ES2-H, ES2-AFS2, June 9, 2017*
- *Nimble Storage Array Installation – Adaptive Flash Quick Start Guide,* Revision A, 05/02/2017
- *Nimble Storage GUI Administration Guide,* Version 4, Published Date: April 20, 2017
- *Nimble Storage CLI Administration Guide,* Version 4, Published Date: April 20, 2017
- *Nimble Storage Command Reference,* Version 4, Published Date: April 20, 2017
- Nimble Storage REST_API_ 4.2.0.1.zip (a collection of HTML files)
- *Nimble Storage, Inc.; NimbleOS v4.2; Guidance Documentation Supplement; Evaluation Assurance Level (EAL); EAL2+; Document version: 0.6 (available only with the TOE link)*

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:

[29] PDF – Portable Document Format

1.5.2.1 Security Audit

The TOE generates audit records for startup and shutdown of the appliance and all administrator-initiated, non-read operations performed on an array through the NimbleOS API, NimbleOS CLI, or NimbleOS GUI. Only TOE administrators with the Administrator role can view the audit records for all administrator-initiated, non-read operations performed on an array. All TOE administrators can view the startup and shutdown events. All TOE administrators are prevented from deleting the audit records. The audit records show the identity of the user that performed the operation.

1.5.2.2 Cryptographic Support

The TOE uses the Nimble Storage, Inc. FIPS Object Module cryptographic module to perform cryptographic operations. These cryptographic operations are used to secure communications from remote administrators at the NimbleOS GUI, API, and CLI. They are also used to encrypt data at rest on selected volumes within an array, protect the keys used for data encryption, and provide X.509 certificates. All cryptographic keys generated by the TOE. Keys are destroyed according to FIPS 140-2 zeroization methods. The master key that encrypts volume keys is zeroized when destroyed.

1.5.2.3 User Data Protection

The TOE enforces the Storage Access Control SFP[30] to control iSCSI and FC client access to Nimble array volumes. An authorized TOE administrator configures this access by setting security attributes using the NimbleOS GUI, CLI, or API. If these security attributes are not configured, clients have no access to volumes on the Nimble arrays.

The Encrypted Volume Access Control SFP ensures that only authorized TOE administrators with the Administrator, Power User, or Operator role can encrypt and replicate volumes, manage iSCSI and FC clients' security attributes, manage volume ACL[31]s, and manage user roles. Once a volume is set as encrypted, it is stored and replicated in an encrypted form.

Data storage integrity is provided with triple+ parity RAID capabilities that monitor checksums on user data for errors. If an error cannot be repaired, the corresponding drive is declared failed.

The TOE provides volume and volume collection snapshot capabilities, allowing for the rollback of a volume or volume collection to the point in time a chosen snapshot was created. All of the operations on a volume can be rolled back.

1.5.2.4 Identification and Authentication

TOE administrator authentication can be performed in multiple ways on the TOE. NimbleOS supports local and AD authentication. All TOE administrators must be identified and authenticated prior to performing any actions at the NimbleOS GUI, API, or CLI. Note that end-users are not authenticated directly by the TOE. They connect to the iSCSI and FC clients, which are restricted access based on the Storage Access Control SFP.

The TOE maintains the following list of security attributes belonging to local user accounts: username, password, and role. The TOE obscures passwords entered at the NimbleOS GUI during authentication using a bullet (•) in place of each character.

[30] SFP – Security Function Policy

[31] ACL – Access Control List. ACLs are collections of either iSCSI or FC initiators that are part of an initiator group.

1.5.2.5 Security Management

The TOE is managed by TOE administrators in one of four roles: Administrator, Power User, Operator, or Guest. The TOE is capable of performing the following management functions: configuring arrays and volumes, configuring NTP, viewing the audit logs, configuring user authentication, performing snapshots and rollbacks, setting access controls, and configuring X.509 certificates for TLS. Only the NimbleOS CLI can be used to configure X.509 certificates. The TOE will restrict access to management functions based on the user's privilege level.

The TOE enforces the Encrypted Volume Access Control SFP to restrict the ability to manage security attributes to TOE administrators with the Administrator, Power User, and Operator role. These security attributes restrict access to NimbleOS arrays by default.

1.5.2.6 Protection of the TOE Security Functionality (TSF)

The TOE is able to preserve a secure state when up to two drives or a single controller on an array fails.

The TOE will provide reliable timestamps that are used for the audit trail. The TOE's time will be synchronized with an NTP server in the TOE environment.

1.5.2.7 Trusted Path/Channels

The TOE provides a trusted channel between itself and another trusted IT product (a replication partner in this case) by making secure connections over TLSv1.2. It uses this trusted channel to transfer wrapping keys that are used to protect volume encryption keys.

Using a supported Web browser, a remote TOE administrator initiates a secure connection to the TOE. The secure path is established using HTTPS for the NimbleOS GUI and NimbleOS API. Using an SSH client, a remote TOE administrator initiates a secure connection to the NimbleOS CLI over SSH. The HTTPS and SSH connections are used to protect data communications from modification or disclosure and ensure end point identification.

2. Conformance Claims

This section and Table 2 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 2 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the CEM as of 2016/10/17 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

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 administrators: 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 administrators are, however, assumed not to be willfully hostile to the TOE.)
- Natural threats: There are threats to the TSF that are a natural byproduct of the systems that compose the TOE, such as electromagnetic interference on a line during transmission of user data.

All agents are assumed to have a low level of motivation. The IT assets requiring protection are the TSF[32] and user data saved on or transitioning through the TOE and the hosts on the protected network. Both the confidentiality and integrity of the data must be protected. Removal, diminution and mitigation of the threats are through the objectives identified in Section 4 Security Objectives. Table 3 below lists the applicable threats.

Table 3 – Threats

Name	Description
T.DATA_CORRUPTION	Data could become corrupted or security functionality compromised due to hardware failure caused by natural threats or incorrect system operations.
T.INTERCEPT	The TOE may communicate with remote IT entities and TOE administrator workstations that lie outside of the organization's trusted network. An attacker who is not a TOE user may attempt to intercept these communications in order to read or modify critical TSF data.
T.UNAUTH	An unauthorized person may gain access to security data on the TOE.
T.UNINTENDED_ACCESS	An attacker who is not a TOE user could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.

[32] TSF – TOE Security Functionality

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. There are no OSPs imposed upon the TOE or its operational environment by any organization implementing the TOE in the CC evaluated configuration.

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 4 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 4 – Assumptions

Name	Description
A.NETWORK	The TOE environment provides the network infrastructure required for management and storage traffic.
A.TIMESTAMP	The IT environment provides the TOE with the necessary reliable timestamps.
A.LOCATE	The TOE, the arrays, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a controlled access facility.
A.PROTECT	The TOE software will be protected from unauthorized modification.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	TOE administrators (Administrator, Power User, Operator, and Guest role) who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.ADMIN_PROTECT	No malicious software is installed or running on the TOE administrator workstation.
A.ENVIRON_ADMIN	There are one or more competent, non-hostile individuals assigned to manage TOE environmental components.

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 5 below.

Table 5 – Security Objectives for the TOE

Name	Description
O.ACCESS	The TOE must implement rules to govern FC and iSCSI client access to stored user data.
O.ADMIN	The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.
O.AUDIT	The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail and provide authorized administrators with the ability to review the audit trail.
O.AUTHENTICATE	The TOE must be able to identify and authenticate TOE administrators (administrators having the Administrator, Power User, Operator, or Guest role) through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. Note that end-users connect to FC and iSCSI clients; they do not authenticate directly to the TOE.
O.PROTECT	The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.
O.TSF_PROTECT	The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when hardware failures occur.
O.USER_DATA_PROTECT	The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized TOE administrator to restore a volume (of user data) to a desired point-in-time. It must also protect user data through encryption of selected volumes and the export of user data with security attributes.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

Table 6 below lists the IT security objectives that are to be satisfied by the environment.

Table 6 – IT Security Objectives

Name	Description
OE.TIME	The TOE environment must provide reliable timestamps to the TOE.
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference or tampering.
OE.NETWORK	The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.
OE.ADMIN_PROTECT	The TOE administrator workstation must be protected from any external interference or tampering.

4.2.2 Non-IT Security Objectives

Table 7 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 7 – 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

There are no extended TOE security functional components defined for this evaluation.

5.2 Extended TOE Security Assurance Components

There are no extended TOE security assurance components defined for this evaluation.

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 within brackets*].
- Completed selection statements are identified using [*italicized and underlined text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- 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 8 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 8 – TOE Security Functional Requirements

Name	***Description***	***S***	***A***	***R***	***I***
FAU_GEN.1	*Audit Data Generation*	✓	✓		
FAU_GEN.2	*User Identity Association*				
FAU_SAR.1	*Audit review*		✓		
FAU_STG.1	*Protected audit trail storage*	✓			
FCS_CKM.1	*Cryptographic key generation*		✓		
FCS_CKM.4	*Cryptographic key destruction*		✓		
FCS_COP.1	*Cryptographic operation*		✓		
FDP_ACC.1(a)	*Subset access control*		✓		
FDP_ACC.1(b)	*Subset access control*		✓		

FDP_ACF.1(a)	*Security attribute based access control*		✓		
FDP_ACF.1(b)	*Security attribute based access control*		✓		
FDP_ETC.2	*Export of user data with security attributes*		✓		
FDP_ROL.2	*Advanced rollback*		✓		
FDP_SDI.2	*Stored data integrity monitoring and action*		✓		
FIA_ATD.1	*User attribute definition*		✓		
FIA_UAU.2	*User authentication before any action*				
FIA_UAU.5	*Multiple authentication mechanisms*		✓		
FIA_UAU.7	*Protected authentication feedback*		✓		
FIA_UID.2	*User identification before any action*				
FMT_MSA.1(a)	*Management of security attributes*	✓	✓		
FMT_MSA.1(b)	*Management of security attributes*	✓	✓		
FMT_MSA.3	*Static attribute initialisation*	✓	✓		
FMT_SMF.1	*Specification of management functions*		✓		
FMT_SMR.1	*Security roles*		✓		
FPT_FLS.1	*Failure with preservation of secure state*		✓		
FPT_STM.1	*Reliable time stamps*				
FTP_ITC.1	*Inter-TSF trusted channel*	✓	✓		
FTP_TRP.1	*Trusted path*	✓			

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. [*administrator-initiated, non-read operations performed on an array*].

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, [*Access Type, Client IP Address, Event Category*].

The alerts generated for audit startup and shutdown are service events. They are not intended to be a success/fail operation; they are generated when system events occur. Therefore, there will not be a success or failure indication for these events. However, the description for the events does provide an outcome (e.g., the startup event states "Service started" indicating the service started.

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_SAR.1 Audit review

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

FAU_SAR.1.1

The TSF shall provide [*authorized TOE administrators*] with the capability to read [*start-up and shutdown event (all TOE administrators); administrator-initiated, non-read operations performed on an array (TOE administrators with the Administrator role only)*] from the audit records.

FAU_SAR.1.2

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

Application Note: The start-up event for the audit function is associated with a start-up alert with ID 2101 issued for the TOE's Group Management Daemon (GMD) process. The shutdown event for the audit function is associated with a shutdown event issued for the TOE's GMD process. All TOE administrators can view the start-up alert and shutdown event from the NimbleOS GUI **Home > Events** menu or NimbleOS CLI `alert --list` command. The audit records for administrator-initiated, non-read operations performed on an array can only be viewed by TOE administrators with the Administrator role via the **Audit Log** page of the NimbleOS GUI by selecting **Monitor > Audit Log**, via the NimbleOS CLI `auditlog` command, or via the NimbleOS API `audit_log` read operation.

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 unauthorized deletion.

FAU_STG.1.2

The TSF shall be able to [*prevent*] unauthorized modifications to the stored audit records in the audit trail.

6.2.2 Class FCS: Cryptographic Support

FCS_CKM.1 Cryptographic key generation

Hierarchical to: No other components.

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*symmetric key generation using a deterministic random bit generator with options for Hash DRBG; HMAC DRBG, no reseed; and CTR DRBG (AES), no derivation or asymmetric key generation using RSA schemes*] and specified cryptographic key sizes [*listed in* Table 9] that meet the following: [*none*].

Table 9 – List of Key Sizes that the TOE can Generate

Key Type	Key Sizes
AES[33] Key	128, 192, 256
RSA[34] Key Pair Gen	2048
HMAC[35] Key	160, 256, 384, 512

FCS_CKM.4 Cryptographic key destruction

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

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 standard zeroization requirements*].

FCS_COP.1 Cryptographic operation

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

FCS_COP.1.1

The TSF shall perform [*list of cryptographic operations listed in Table 10*] in accordance with a specified cryptographic algorithm [*listed in Table 10*] and cryptographic key sizes [*listed in Table 10*] that meet the following: [*list of standards (Certificate #) in Table 10*].

[33] AES – Advanced Encryption Standard

[34] RSA – *Rivest-Shamir-Adleman*

[35] HMAC – Keyed-Hash Message Authentication Code

Table 10 – Cryptographic Operations

Cryptographic Operations	Cryptographic Algorithm	Key/Digest Size (bits)	Certificate #
Symmetric Encryption and Decryption	AES (CBC[36], CTR[37], GCM[38], XTS)	128, 192, 256	2484, 3351
Message Digest	SHA[39]-1 SHA-2	SHA-1 (160) SHA-2 (256, 384, 512)	2102, 2778
Keyed Hash	HMAC with SHA-1, SHA-2	SHA-1 (160) SHA-2 (256, 384, 512)	1526, 2134
Digital Signature Generation and Verification	RSA	2048, with all SHA-2 sizes	1273, 1718
ECC[40] CDH[41] (CVL[42])	All NIST[43] defined P curves except 192	224, 256, 384, 521	85, 496

6.2.3 Class FDP: User Data Protection

FDP_ACC.1(a) 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 [*Storage Access Control SFP*] on [
Subjects: iSCSI and FC clients
Objects: Volumes
Operations: Read and Write
].

FDP_ACC.1(b) 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 [*Encrypted Volume* access *control SFP*] on [

- *Subjects: TOE administrators with the Administrators, Power User, or Operator role*
- *Objects: Volumes, user roles, iSCSI and FC clients*

[36] CBC – Cipher Block Chaining
[37] CTR – Counter Mode
[38] GCM – Galois Counter Mode
[39] SHA – Secure Hash Algorithm
[40] ECC – Elliptic Curve Cryptography
[41] CDH – Cofactor Diffie-Hellman
[42] CVL – Component Validation List
[43] NIST – National Institute of Standards and Technology

- *Operations: encrypt and replicate volumes, manage volume ACL[44]s, user roles, and iSCSI and FC client security attributes*

].

FDP_ACF.1(a) 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 [*Storage Access Control SFP*] to objects based on the following: [

1) iSCSI client SFP-relevant security attributes:
   - IQN Initiators
   - Username for CHAP authentication (i.e., account name defined on volume)
   - Initiator Secret for CHAP authentication
   - Access control record (for CHAP target authentication)

2) FC client SFP-relevant security attributes:
   - WWPN Initiators

3) Volume SFP-relevant security attributes:
   - Target Secret for CHAP authentication
   - iSCSI Initiator Group
   - FC Initiator Group
   - Volume ID
   - Account Name (i.e., iSCSI client username)
   - Access control record (for CHAP initiator authentication)
   - ACL

].

FDP_ACF.1.2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*An iSCSI client can access a volume to perform read/write operations if 1) CHAP authentication is successful and/or 2) its initiator IQN is in the ACL defined for the volume. A FC client has similar access to a volume if its initiator WWPN is in the ACL defined for the volume*].

FDP_ACF.1.3

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

FDP_ACF.1.4

The TSF shall explicitly deny access of subjects to objects based on the [*no other rules*].

FDP_ACF.1(b) Security attribute based access control

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

[44] ACL – Access Control List. ACLs are collections of either iSCSI or FC initiators that are part of an initiator group.

FDP_ACF.1.1

The TSF shall enforce the [*Encrypted Volume access control SFP*] to objects based on the following: [

- *Subject attributes: Role*
- *Object attributes: Volume ID*[45]*, volume ACLs, user roles, iSCSI client security attributes (CHAP accounts, iSCSI initiator groups, and FC client security attributes (FC initiator groups)*].

FDP_ACF.1.2

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

- *If a subject's role has the required privilege, that subject is permitted to encrypt or replicate volumes and manage volume ACLs, user roles, and iSCSI and FC client security attributes].*

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_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1

The TSF shall enforce the [*Encrypted Volume access control SFPs*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3

The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [*volume data that has been encrypted must be exported encrypted*].

FDP_ROL.2 Advanced rollback

Hierarchical to: FDP_ROL.1 Basic rollback
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]

FDP_ROL.2.1

The TSF shall enforce [*Storage Access Control SFP*] to permit the rollback of all the operations on the [*data located in storage volumes*].

FDP_ROL.2.2

The TSF shall permit operations to be rolled back within the [*period of time since a chosen snapshot was created*].

[45] ID - Identifier

FDP_SDI.2 Stored data integrity monitoring and action

Hierarchical to: FDP_SDI.1 Stored data integrity monitoring

Dependencies: No dependencies

FDP_SDI.2.1

The TSF shall monitor user data stored in containers controlled by the TSF for [*integrity errors*] on all objects, based on the following attributes: [*checksum associated with the data*].

FDP_SDI.2.2

Upon detection of a data integrity error, the TSF shall [*attempt to repair the data from a known good copy and declare the drive failed if the repair is not possible*].

6.2.4 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_ATD.1.1

The TSF shall maintain the following list of security attributes belonging to individual users: [*username, role, and password for local authentication; AD groups and associated roles for AD authentication*].

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2.1

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

FIA_UAU.5 Multiple authentication mechanisms

Hierarchical to: No other components.

Dependencies: No dependencies

FIA_UAU.5.1

The TSF shall provide [*local and AD authentication mechanisms*] to support user authentication.

FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*username and password provided by user matches that in distributed database (for local authentication) or AD (for AD authentication)*].

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1

The TSF shall provide only [*obscured feedback via the NimbleOS GUI*] 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.

6.2.5 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1

The TSF shall enforce the [*Storage Access Control SFP*] to restrict the ability to [*query, modify, delete, [add]*] the security attributes [*CHAP credentials, iSCSI and FC initiator groups, volume ACLs*] to [*TOE administrators with the Administrator, Power User, or Operator role*].

FMT_MSA.1(b) Management of security attributes

Hierarchical to: No other components.

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

FMT_MSA.1.1

The TSF shall enforce the [*Encrypted Volume Access Control SFP*] to restrict the ability to [*query, modify, delete, [add]*] the security attributes [*role*] to [*authorized administrators*].

FMT_MSA.3 Static attribute initialization

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 [*Encrypted Volume Access Control SFP and Storage 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 [*TOE administrators with Administrator, Power User, or Operator role*] 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: [*configuring arrays and volumes, configuring NTP, viewing the audit logs, configuring user authentication, performing snapshots and rollbacks, setting access controls, and configuring X.509 certificates*].

Application note: Only the NimbleOS CLI may be used to configure X.509 certificates.

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 [*Administrator, Power User, Operator, and Guest*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

6.2.6 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: [*up to 2 drive failures or a single controller failure on an array*].

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.
Dependencies: No dependencies

FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

6.2.7 Class FTP: Trusted Path/Channels

FTP_ITC.1 Inter-TSF trusted channel

Hierarchical to: No other components.
Dependencies: No dependencies

FTP_ITC.1.1

The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1.2

The TSF shall permit [*the TSF*] to initiate communication via the trusted channel.

FTP_ITC.1.3

The TSF shall initiate communication via the trusted channel for [*transfer of wrapping keys to replication partners*].

FTP_TRP.1 Trusted path

Hierarchical to: No other components.
Dependencies: No dependencies

FTP_TRP.1.1

The TSF shall provide a communication path between itself and [*remote*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [*modification, disclosure*].

FTP_TRP.1.2

The TSF shall permit [*remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3

The TSF shall require the use of the trusted path for [initial user authentication, *[HTTPS connections to the NimbleOS GUI and NimbleOS API, SSH connections to the NimbleOS CLI]*].

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 augmented with ALC_FLR.2. Table 11 – Assurance Requirements summarizes these requirements.

Table 11 – 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[46] 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 Analysis of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

[46] CM – Configuration Management

7. TOE Summary 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 12 lists the security functions and their associated SFRs.

Table 12 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
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(a)	Subset access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_ETC.2	Export of user data with security attributes
	FDP_ROL.2	Advanced rollback
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.2	User authentication before any action
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1(a)	Management of security attributes

	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1	Security roles
Protection of TOE Security Functionality	FPT_STM.1	Reliable time stamps
	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Trusted Path/Channels	FTP_ITC.1	Inter-TSF trusted channel
	FTP_TRP.1	Trusted path

7.1.1 Security Audit

The TOE generates audit records for start-up and shutdown of the appliance and all administrator-initiated, non-read operations performed on the array through the NimbleOS API, CLI, or GUI.

The start-up event for the audit function is associated with a start-up alert with ID 2101 issued for the TOE's Group Management Daemon (GMD) process. The shutdown event for the audit function is associated with a shutdown event issued for the TOE's GMD process. Since these events are service events, they are not intended to be a success/fail operation. Their description does, however, provide an outcome. The startup event associated with the GMD process has a description indicating "Service started". The shutdown event associated with the GMD process has a description indicating "Halting controller <> on user request".

All TOE administrators can view the start-up alert and shutdown event from the NimbleOS GUI **Home > Events menu** or NimbleOS CLI `alert --list` command.

The audit records for administrator-initiated, non-read operations performed on an array can only be viewed by administrators with the Administrator role via the **Audit Log** page of the NimbleOS GUI by selecting **Monitor > Audit Log**, the NimbleOS CLI `auditlog` command, or the NimbleOS API `audit_log` read operation. All TOE administrators are prevented from deleting the audit records. The audit records show the identity of the user that performed the operation.

The TOE audit records contain the following information:

Table 13 – Audit Record Contents

Field	Content
Type	Unique ID associated with a particular audit log record
Operation Type	Type of operation (i.e., Create, Update, Delete, or Other)
Event Category	Category of administrator-initiated action (i.e., Data Access, System Configuration, User Access, Data Provisioning, Software Updated, or Data Protection)
Activity	Message associated with the event indicating the type of event

Field	Content
Status	Outcome of the event
Access Type	Type of access audited (i.e., NimbleOS API, CLI, or GUI)
Client IP Address	IP address of client where action was invoked
Username	Subject identity
Time	Date and time of the event

The type of event is indicated by the message provided in the "Activity" field. In addition, the NimbleOS GUI records can be filtered by activity category; thereby indicating the category. The NimbleOS CLI `auditlog` command has options for specifying category, access type, and info (which provides Client IP): `auditlog –access_type, auditlog –category, and auditlog –info <unique ID>`.

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

7.1.2 Cryptographic Support

The TOE uses the Nimble Storage, Inc. FIPS Object Module cryptographic module to perform the cryptographic operations listed in Table 10.

The Nimble Storage, Inc. FIPS Object Module resides in the NimbleOS and is used to provide the following functionality:

- Secure communications from remote users (TOE administrators) to the NimbleOS GUI and NimbleOS API using HTTPS and to the NimbleOS CLI using SSH – relies on the symmetric encryption and decryption cryptographic operations, HMAC with SHA-1 or SHA-2 for integrity, and ECC CDH or RSA for key exchange
- Encryption of data at rest on selected volumes within an array using the AES XTS with 256-bit keys encryption algorithm – uses the AES XTS cryptographic operations
- Protection of keys used for data encryption, at rest and in transit (AES-256-KeyWrap)
- X.509 certificate management for TLS – uses the RSA digital signature generation and verification cryptographic operations with a SHA hash
- Integrity of the Nimble Storage, Inc. FIPS Object Module is verified using an HMAC-SHA-1 hash

The TOE uses the Nimble Storage, Inc. FIPS Object Module to generate the asymmetric and symmetric keys with key sizes as listed in Table 9. The keys are generated by a deterministic random bit generator with options for Hash DRBG; HMAC DRBG, no reseed; and CTR DRBG (AES), no derivation *(CAVP certificate numbers 342 and 784)*. Asymmetric key generation is performed using [FIPS 186-3] RSA (CAVP certificate numbers 1273 and 1718). The TOE uses RSA signature generation and verification. The cryptographic module is completely contained within the TOE boundary and contains all instructions to generate and zeroize cryptographic keys.

The TOE destroys the master encryption key by overwriting it with zeros based on FIPS 140-2 zeroization methods. All volume keys are encrypted with the master key and stored in a key store. Once the master key is zeroized the volume keys cannot be decrypted. Session keys are ephemeral and are destroyed when the session ends. All algorithms and certificate numbers are listed above in Table 10.

The cryptographic module is completely contained within the TOE boundary and contains all instructions to generate and zeroize cryptographic keys. The TOE destroys all keys by overwriting them with zeros based on FIPS 140-2 zeroization methods.

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

7.1.3 User Data Protection

The TOE enforces the Storage Access Control SFP to control iSCSI and FC client access to Nimble array volumes. An authorized administrator configures this access by setting security attributes (e.g., CHAP credentials, IQNs/WWPNs, ACLs) via the NimbleOS GUI, CLI, or API. If these security attributes are not configured, clients have no access to volumes on the Nimble arrays. The TOE enforces access control to hosted volumes using accounts (CHAP authentication) and ACLs.

Account-based access control works in conjunction with ACLs. For account-based access control, a volume is assigned an ACL with the iSCSI client's IQN along with a CHAP account with the username of the iSCSI client to whom authorized access will be granted and associated CHAP credentials. Through an IP connection to the array, an iSCSI client can access a volume to perform read/write operations if CHAP authentication is successful. For authentication to succeed, the iSCSI client username and password (initiator secret) must match that assigned to the volume. If bidirectional CHAP is configured, then the target (volume) must also authenticate with the initiator (iSCSI client). In this case, the iSCSI client must have a record of the username and password (target secret) for the volume(s) being accessed.

ACLs provide access control between a list of iSCSI initiator IQNs or FC WWPNs and an associated group of volumes. ACLs may contain volumes from more than one account. Each iSCSI initiator IQN that is added to an ACL can securely access each volume to which the ACL is assigned without requiring CHAP authentication. Each FC WWPN that is added to an ACL will allow FC network access from that WWPN to the volumes assigned that ACL.

The Encrypted Volume access control SFP ensures that only TOE administrators with the Administrator, Power User, or Operator role can encrypt or replicate volumes and manage volume ACLs, user roles, and iSCSI and FC client security attributes. It allows TOE administrators with the proper privilege to set a volume as encrypted, so that the data with the volume is stored in an encrypted form. The TOE ensures that encrypted data remains encrypted when replicated. In addition, the TOE sends a checksum with all replicas (or copies of volumes) exported to ensure that the content is consistent between replication partners.

Data storage integrity is provided with monitoring of checksums using triple-parity RAID capabilities. The TOE monitors checksums on user data to check for data integrity errors. If an error is encountered, the TOE will attempt to repair the data from a known good copy or declare the drive failed if the repair is not possible.

The TOE provides volume and volume collection snapshot capabilities, allowing for the rollback of all the operations on a volume or volume collection to a point in time a chosen snapshot was created.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACF.1(a), FDP_ACC.1(b), FDP_ACF.1(b), FDP_ETC.2, FDP_ROL.2, FDP_SDI.2

7.1.4 Identification and Authentication

TOE administrator authentication can be performed in multiple ways on the TOE. NimbleOS supports both local and AD authentication.

With local authentication, TOE administrators are authenticated using a local password-based mechanism, which authenticates and authorizes them based on their username, password, and role attributes, which are stored in a database. For AD authentication, the TOE uses an AD server in the TOE environment to authenticate TOE administrators. All NimbleOS GUI, CLI, and API actions require a valid username and password combination upon invocation. As passwords are entered at the NimbleOS GUI, the characters are masked with bullets. No functionality is available to a TOE administrator prior to authentication. A successful login provides the TOE administrator the roles and capabilities within the NimbleOS GUI, API, and CLI as defined by user accounts.

TOE Security Functional Requirements Satisfied: FIA_ATD.1, FIA_UAU.2, FIA_UAU.5, FIA_UAU.7, FIA_UID.2

7.1.5 Security Management

The TOE is managed by TOE administrators in one of four roles: Administrator, Power User, Operator, or Guest. The TOE provides TOE administrators with the Administrator role full privileges including the ability to create and manage user accounts for other users. A TOE administrator with the Power User role can perform all functions except user management, inactivity timeout, and array setup and re-setup. A TOE administrator with the Operator role can perform all functions except data deletion and removal. A TOE administrator with the Guest role has read-only capabilities.

The TOE enforces the Encrypted Volume Access Control SFP to restrict the ability to manage security attributes (CHAP credentials, iSCSI and FC initiator groups, volume ACLs) to TOE administrators with the Administrator, Power User, and Operator role. These security attributes restrict access to NimbleOS arrays by default.

The TOE is capable of performing the following management functions: configuring arrays and volumes, configuring NTP, viewing the audit logs, configuring user authentication, performing snapshots and rollbacks, setting access controls, and configuring X.509 certificates for TLS. Only the NimbleOS CLI may be used to configure X.509 certificates for TLS.

TOE Security Functional Requirements Satisfied: FMT_MSA.1(a), FMT_MSA.1(b), FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

7.1.6 Protection of the TSF

The TOE is able to preserve a secure state when up to two drives or a single controller on an array fail. The TOE leverages its triple+ parity RAID to protect against up to three simultaneous complete drive failures. The TOE monitors for controller failures and provides controller failover capability by instantly mirroring data from an active to a standby controller NVRAM.

Through a networked connection to an external NTP server, the TOE periodically synchronizes its time to an external time source. Once the TOE obtains the time from the NTP server, it maintains this time internally and uses it to provide reliable time stamps for auditing.

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

7.1.7 Trusted Path/Channels

The TOE provides a trusted channel between itself and replication partners by making secure connections over TLSv1.2. It uses this trusted channel to transfer wrapping keys that are used to protect volume encryption keys. Only the TOE is allowed to initiate this secure channel communications.

Using a supported Web browser, a remote TOE administrator initiates a secure connection to the TOE. The secure path is established using HTTPS for the NimbleOS GUI and NimbleOS API. Using an SSH client, a remote TOE administrator initiates a secure connection to the NimbleOS CLI over SSH. The HTTPS and SSH connections are used to protect data communications from modification or disclosure and ensure end point identification.

TOE Security Functional Requirements Satisfied: FTP_ITC.1, FTP_TRP.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 Release 4.

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 14 below provides a mapping of the objectives to the threats they counter.

Table 14 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION Data could become corrupted or security functionality compromised due to hardware failure caused by natural threats or incorrect system operations.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	O.ADMIN supports the mitigation of this threat by ensuring that only authorized users may configure the TOE security mechanisms.
	O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail and provide 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.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when hardware failures occur.	O.TSF_PROTECT mitigates this threat by providing mechanisms to protect the TOE data from unauthorized modification.

	O.USER_DATA_PROTECT The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized TOE administrator to restore a volume (of user data) to a desired point-in-time. It must also protect user data through encryption of selected volumes and the export of user data with security attributes.	The objective O.USER_DATA_PROTECT mitigates this threat by monitoring user data for errors, encrypting user data, allowing rollbacks to a point-in-time, and the export of user data with security attributes.
	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.INTERCEPT The TOE may communicate with remote IT entities and TOE administrator workstations that lie outside of the organization's trusted network. An attacker who is not a TOE user may attempt to intercept these communications in order to read or modify critical TSF data.	O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	The objective O.PROTECT ensures that the TOE ensures the integrity of TSF data by protecting itself from unauthorized modifications and access by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems, remote users, and physically separated parts of the TOE.
T.UNAUTH An unauthorized person may gain access to security data on the TOE.	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) 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.AUTHENTICATE The TOE must be able to identify and authenticate TOE administrators (administrators having the Administrator, Power User, Operator, or Guest role) through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. Note that end-users connect to FC and iSCSI clients; they do not authenticate directly to the TOE.	The objective O.AUTHENTICATE ensures that TOE administrators are identified and authenticated prior to gaining any access to TOE security data.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when hardware failures occur.	The objective O.TSF_PROTECT mitigates this threat by ensuring TSF functions that monitor access continue to operate in the event of hardware failures.

T.UNINTENDED_ACCESS An attacker who is not a TOE user could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.	O.ACCESS The TOE must implement rules to govern FC and iSCSI client access to stored user data.	This objective O.ACCESS ensures only authorized iSCSI and FC clients obtain access to TOE storage.
	O.ADMIN The TOE must include a set of functions that allow efficient management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.	The objective O.ADMIN ensures that only authorized TOE administrators have access to TOE security data and management functionality.
	O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail and provide 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.AUTHENTICATE The TOE must be able to identify and authenticate TOE administrators (administrators having the Administrator, Power User, Operator, or Guest role) through multiple authentication mechanisms prior to allowing any access to TOE administrative functions and TSF data. Note that end-users connect to FC and iSCSI clients; they do not authenticate directly to the TOE.	The objective O.AUTHENTICATE ensures that TOE administrators are identified and authenticated prior to gaining any access to TOE security data.
	O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when hardware failures occur.	The objective O.TSF_PROTECT mitigates this threat by ensuring continued operation of TOE in a secure state in the event of hardware failures.

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

There are no Organizational Security Policies defined for this Security Target.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 15 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 15 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.NETWORK The TOE environment provides the network infrastructure required for management and storage traffic.	OE.NETWORK The TOE environment must be implemented such that the TOE is appropriately located within the network to perform its intended function.	OE.NETWORK satisfies the assumption that the TOE environment will provide the appropriate connectivity to allow the TOE to perform its function.
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.
A.LOCATE The TOE, the arrays, storage clients, switches, storage and management networks, firewall, and NTP and LDAP servers are located within a 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.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.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.NOEVIL TOE administrators (Administrator, Power User, Operator, and Guest role) who manage the TOE 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.ADMIN_PROTECT No malicious software is installed or running on the TOE administrator workstation.	OE.ADMIN_PROTECT The TOE administrator workstation must be protected from any external interference or tampering.	OE.ADMIN_PROTECT satisfies the assumption by ensuring that the TOE administrator workstation is protected from external interference or tampering.
A.ENVIRON_ADMIN There are one or more competent, non-hostile individuals assigned to manage TOE environmental components.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference or tampering.	OE.PROTECT satisfies the assumpti0on that the TOE environmental components are managed by competent, non-hostile administrators.

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

There are no extended Security Functional Requirements in this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended TOE Security Assurance Requirements 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 16 below shows a mapping of the objectives and the SFRs that support them.

Table 16 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS The TOE must implement rules to govern FC and iSCSI client access to stored user data.	FDP_ACC.1(a) Subset access control	The requirement meets the objective by ensuring that the Storage Access Control SFP is applied to all storage connection attempts by FC and iSCSI clients.
	FDP_ACF.1(a) Security attribute based access control	The requirement meets the objective by ensuring that the TOE enforces the Storage Access Control SFP on all storage connection attempts by FC and iSCSI clients.
	FMT_MSA.1(a) Management of security attributes	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.3 Static attribute initialisation	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.
O.ADMIN The TOE must include a set of functions that allow efficient	FMT_MSA.1(a) Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts management of security attributes to only

management of its functions, security attributes, and TSF data, ensuring that only authorized TOE administrators (in defined roles) may exercise such control.		those users with the appropriate privileges.
	FMT_MSA.1(b) Management of security attributes	The requirement meets the objective by ensuring that the TOE restricts management of security attributes to only those users with the appropriate privileges.
	FMT_MSA.3 Static attribute initialisation	The requirement meets the objective by ensuring that the TOE restricts administrative functions to only those users with the appropriate privileges.
	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, security attributes, and TSF data.
O.AUDIT The TOE must record security relevant events and associate each event with the identity of the user that caused the event. The TOE must prevent unauthorized modification of the audit trail and provide authorized administrators with the ability to review the audit trail.	FAU_GEN.1 Audit Data Generation	The requirement meets the 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	This requirement meets the objective by ensuring user actions are associated with the administrator that invoked the event.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides authorized administrators the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FPT_STM.1 Reliable time stamps	The requirement meets the objective by providing reliable time stamps for audit records.
O.AUTHENTICATE The TOE must be able to identify and authenticate TOE administrators (administrators having the Administrator, Power User, Operator, or Guest role) through multiple authentication mechanisms prior to allowing any	FIA_ATD.1 User attribute definition	The requirement meets the objective by storing administrators' security attributes that are used for identification and authentication.
	FIA_UAU.2 User authentication before any action	The requirement meets the objective by ensuring each TOE administrator is successfully authenticated before being allowed access to any TSF functionality.

access to TOE administrative functions and TSF data. Note that end-users connect to FC and iSCSI clients; they do not authenticate directly to the TOE.	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by providing both local and LDAP authentication mechanisms.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by obscuring feedback through the NimbleOS GUI during authentication.
	FIA_UID.2 User identification before any action	The requirement meets the objective by ensuring that each TOE administrator is identified before being allowed access to any TSF functionality.
O.PROTECT The TOE must ensure the integrity of system data by protecting itself from unauthorized modifications and access to its functions and data.	FCS_CKM.1 Cryptographic key generation	The requirement meets this objective by ensuring that cryptographic keys created for use by the TOE meet recommended standards for secure generation.
	FCS_CKM.4 Cryptographic key destruction	The requirement meets the objective by ensuring that cryptographic keys no longer in use by the TOE are destroyed via recommended standard key destruction methods.
	FCS_COP.1 Cryptographic operation	The requirement meets the objective by ensuring that the TOE uses recommended standards for all cryptographic functionality implemented to secure communications with trusted remote IT systems, remote users, and physically separated parts of the TOE.
	FIA_UAU.2 User authentication 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 authenticated users are allowed access to all TOE functions.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by preventing password material from being obtained from an unauthorized person, thus protecting from unauthorized access.
	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 all TOE functions.
	FTP_ITC.1 Inter-TSF trusted channel	The requirement meets the objective by providing a secure and trusted communications channel between trusted IT products and the TOE.

	FTP_TRP.1 Trusted path	The requirement meets the objective by providing a secure communications path to all users accessing the TOE remotely.
O.TSF_PROTECT The TOE must protect its functions and TSF data to ensure its SFRs are enforced and capabilities intact when hardware failures occur.	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring the TOE preserves a secure state upon defined hardware failures.
O.USER_DATA_PROTECT The TOE must ensure the integrity of stored user data by monitoring for errors and providing the means for an authorized TOE administrator to restore a volume (of user data) to a desired point-in-time. It must also protect user data through encryption of selected volumes and the export of user data with security attributes.	FCS_COP.1 Cryptographic operation	The requirement meets the objective by providing encryption of user data on selected volumes.
	FDP_ACC.1(b) Subset access control	This requirement meets the objective by allowing users in authorized roles to configure protection schedules for the export of user data.
	FDP_ACF.1(b) Security attribute based access control	This requirement meets the objective by allowing users in authorized roles to configure protection schedules for the export of user data.
	FDP_ETC.2 Export of user data with security attributes	This requirement meets the objective by allowing for the export of user data with security attributes.
	FDP_ROL.2 Advanced rollback	The requirement meets the objective by permitting rollbacks of all the operations on volumes to defined points-in-time (snapshots).
	FDP_SDI.2 Stored data integrity monitoring and action	The requirement meets the objective by ensuring user data is monitored for integrity errors.

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. The TOE 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 TOE 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 17 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 17 – Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UID.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FCS_CKM.1	FCS_CKM.4	✓	
	FCS_COP.1	✓	
FCS_CKM.4	FCS_CKM.1	✓	
FCS_COP.1	FCS_CKM.4	✓	
	FCS_CKM.1	✓	
FDP_ACC.1(a)	FDP_ACF.1(a)	✓	
FDP_ACC.1(b)	FDP_ACF.1(b)	✓	
FDP_ACF.1(a)	FDP_ACC.1(a)	✓	
	FMT_MSA.3	✓	
FDP_ACF.1(b)	FDP_ACC.1(b)	✓	
	FMT_MSA.3	✓	
FDP_ETC.2	FDP_ACC.1(b)	✓	
FDP_ROL.2	FDP_ACC.1	✓	
FDP_SDI.2	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FIA_ATD.1	No dependencies	✓	
FIA_UAU.2	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.5	No dependencies	✓	
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not included, FIA_UAU.2,

			which is hierarchical to FIA_UAU.1 is included. This satisfies this dependency.
FIA_UID.2	No dependencies	✓	
FMT_MSA.1(a)	FDP_ACC.1(a)	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.1(b)	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1(b)	✓	
FMT_MSA.3	FMT_SMR.1	✓	
	FMT_MSA.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.
FPT_FLS.1	No dependencies	✓	
FPT_STM.1	No dependencies	✓	
FTP_ITC.1	No dependencies	✓	
FTP_TRP.1	No dependencies	✓	

9. Acronyms

Table 18 defines the acronyms used throughout this document.

Table 18 – Acronyms

Acronym	Definition
AD	Active Directory
ACL	Access Control List
AES	Advanced Encryption Standard
API	Application Programming Interface
BGL	Backup Group Leader
CASL	Cache Accelerated Sequential Layout
CBC	Cipher Block Chaining
CC	Common Criteria
CDH	Cofactor Diffie-Hellman
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CM	Configuration Management
CVL	Component Validation List
CTR	Counter Mode
DRBG	Deterministic Random Number Generator
EAL	Evaluation Assurance Level
EAR	Encryption at Rest
ECC	Elliptic Curve Cryptography
FC	Fibre Channel
FIPS	Federal Information Processing Standard
GbE	Gigabit Ethernet
GCM	Galois Counter Mode
GL	Group Leader
GMD	Group Management Daemon
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	Keyed-Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier

Acronym	Definition
IE	Internet Explorer
IQN	iSCSI Qualified Name
iSCSI	Internet Small Computer System Interface
IP	Internet Protocol (Address)
IT	Information Technology
LAN	Local Area Network
MAC	Message Authentication Code
NI	New Instruction
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NVRAM	Non-Volatile Random-Access Memory
OS	Operating System
OSP	Organizational Security Policy
PDF	Portable Document Format
PP	Protection Profile
R2	Release 2
RAID	Redundant Array of Independent Disks
RBAC	Role Based Access Control
REST	Representational State Transfer
RSA	Rivest-Shamir-Adleman
RU	Rack Unit
SAN	Storage Area Network
SAR	Security Assurance Requirement
SHA	Secure Hash Algorithm
SMBv2	Server Message Block version 2
SFP	Security Function Policy
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SSD	Solid State Drive
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy

Acronym	Definition
U	Unit
WAN	Wide Area Network
WWPN	World Wide Port Name
XOR	Exclusive Or
XTS	XEX(XOR Encrypt XOR) Tweakable block cipher with ciphertext Stealing

Prepared by:
Corsec Security, Inc.

Corsec

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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