Dell EMC™ VxRail™ 4.7

Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2093-000-D102
Version: 1.6
25 June 2020

Dell EMC
176 South Street
Hopkinton, Massachusetts, USA
01748

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

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

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

1.1 DOCUMENT ORGANIZATION

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

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

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

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

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

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

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

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

1.2 SECURITY TARGET REFERENCE

ST Title:	Dell EMC™ VxRail™ 4.7 Security Target
ST Version:	1.6
ST Date:	25 June 2020

1.3 TOE REFERENCE

TOE Identification: Dell EMC™ VxRail™ 4.7.511-26539430

TOE Developer: Dell EMC

TOE Type: Hyper-converged appliance (other devices and systems)

1.4 TOE OVERVIEW

VxRail is a hyper-converged appliance. Hyper-convergence is a software-defined infrastructure system characterized by tightly integrated compute, storage, networking and virtualization resources.

VxRail is based on VMware vSphere and vSAN software, and built on Dell PowerEdge hardware. vSAN software defines storage that pools the internal disks of industry standard servers to provide integrated, high speed Virtual Machine (VM) storage. VxRail is a fully engineered, turnkey appliance designed as an Infrastructure as a Service (IaaS) platform and foundational infrastructure for Platform as a Service (PaaS) solutions.

VxRail provides the following storage, virtualization and security functionality:

Storage

VMware vSAN is integrated in the VxRail Appliance to provide Software-Defined Storage (SDS). vSAN is not a Virtual Storage Appliance (VSA), but is embedded in the ESXi hypervisor kernel's Input/Output (I/O) data path. vSAN pools the VxRail Appliance's internal Solid State Drives (SSDs) and Hard Disk Drives (HDDs) on the ESXi hosts to present a single datastore for all hosts in the cluster. vSAN uses a distributed, object-based architecture, and distributes the individual virtual disk across the datastore.

Virtualization

VxRail allows virtualization infrastructure administrators to manage resources on a per-VM basis. Policies can be defined at VM-level granularity for provisioning and load balancing. vSAN is fully integrated with vSphere, which simplifies setting up the availability, capacity, and performance policies.

Security

VxRail provides the following security functionality:

- Security audit generation, review and secure storage of audit records
- Monitoring of system health
- Encryption of data at rest
- Assurance of data integrity, and deduplication in support of these services
- Identification and authentication of administrative users
- Secure management through VxRail Manager

- Timeout of inactive administrative sessions

The TOE is a combined software and hardware TOE.

1.4.1 TOE Environment

The following network components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Administrator Workstation	Windows 10	General Purpose Computer Hardware
Key Management	Not applicable	Cloudlink
Network Time Protocol Service	Not applicable	Not applicable

Table 1 – Non-TOE Hardware and Software

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE is the VxRail appliance with 13G/14G hardware and the VxRail Manager 4.7.511 software. The deployment configuration and TOE boundary are shown in Figure 1.

The evaluated configuration includes the VxRail E460F (13G) and E560F (14G) hardware models.

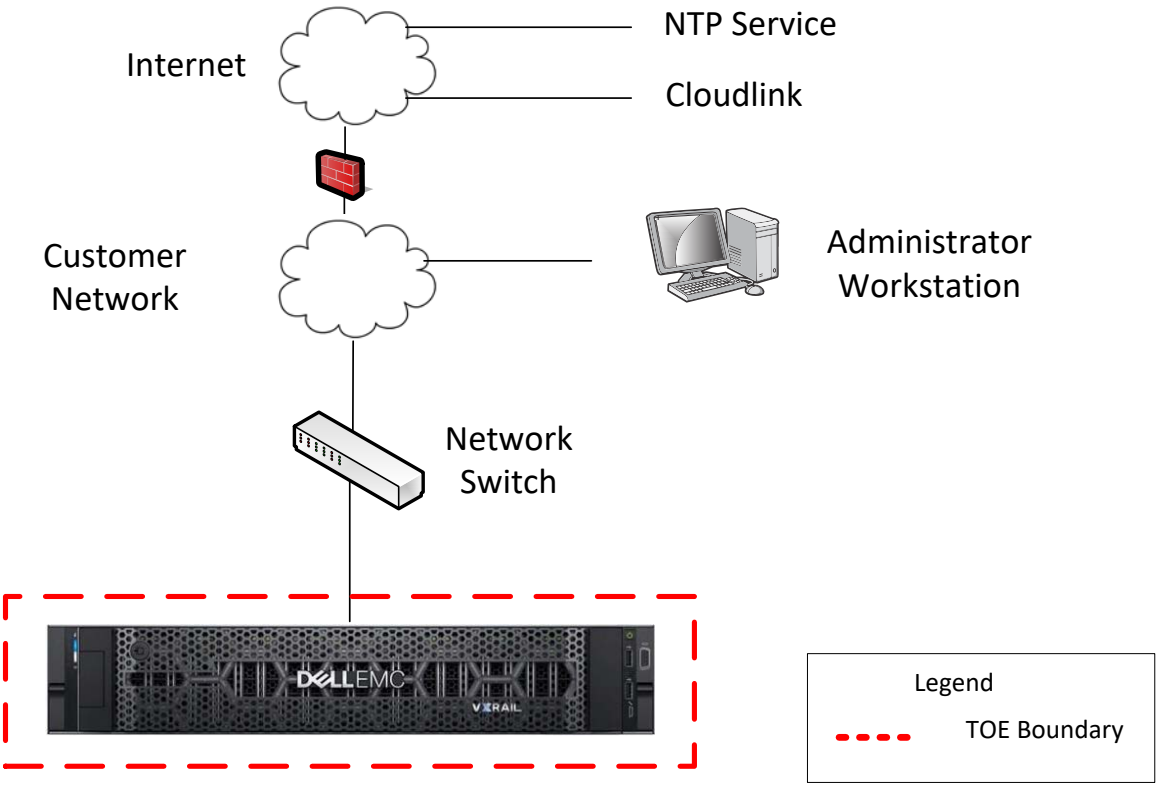

Figure 1 – TOE Diagram

1.5.1.1 TOE Delivery

The TOE is the VxRail E460F and E560F appliances.

The TOE software is installed on the TOE hardware and delivered to the customer by a commercial courier service with a package tracking system. Once delivered, the TOE must be installed by the Dell EMC Professional Services team.

1.5.1.2 TOE Guidance

The TOE includes the following guidance documentation. The documents may be downloaded from the Dell EMC support website in the indicated format:

- Dell EMC VxRail™ Appliance Version 4.7.x Administration Guide, REV 01, published December 2018
  - docu91466_VxRail-Appliance-4.7-Administration-Guide.pdf
- VxRail™ Appliance Version 4.5.x Security Configuration Guide, REV 01, published March 2018
  - docu88405_VxRail-Appliance-Software-4.5.x-Security-Configuration-Guide.pdf
- Dell EMC VxRail™ Appliance Version 4.5. x and 4.7.x API User Guide, REV 02, published January 2019
  - docu91468_VxRail-Appliance-4.5.x-and-4.7.x-API- Guide.pdf

1.5.2 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. The audit logs are protected from unauthorized modification and deletion and the newest records are protected from loss when the audit trail becomes full. Audit records may be sorted reviewed by authorized administrators. Timestamp information is provided to support auditing. Administrators are alerted to potential security issues.
Cryptographic Support	Cryptographic functionality is provided to protect the confidentiality of user data at rest.
User Data Protection	Duplicate data is removed prior to storage. User data is monitored for integrity errors, and correctable errors are fixed when found.
Identification and Authentication	Users must identify and authenticate prior to TOE access. Passwords are obscured as they are entered.
Security Management	The TOE provides management capabilities via a Web-Based Graphical User Interface (GUI) and a Representational State Transfer (REST) Application Programming Interface (API), accessed via Hypertext Transfer Protocol Secure (HTTPS), and a Command Line Interface (CLI) accessed locally. Management functions allow the administrators to manage system health and review audit records.
Protection of the TSF	A secure state is maintained in the case of disk or node failure. Reliable timestamps are provided for audit records.
Resource Utilization	The TOE ensures continued operation in the case of disk or node failure.
TOE Access	Administrative users may log out of an interactive session at any time. Inactive sessions are closed after 30 minutes of inactivity.

Table 2 – Logical Scope of the TOE

1.5.3 Functionality Excluded from the Evaluated Configuration

1.5.3.1 Excluded Services

The following services must not be enabled (disabled by default) and are excluded from the evaluated configuration:

- SRS VE
- VMCloudware VCF

1.5.3.2 Excluded Interfaces

In the evaluated configuration, VxRail is managed from the VxRail GUI, the REST API or the Linux Shell. Direct access to VMware interfaces or individual Virtual Machines (VMs) is outside the scope of this evaluation. These interfaces are not disabled, but should not be used in the evaluated configuration.

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

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

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

As follows:

- CC Part 2 extended
- CC Part 3 conformant

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

2.2 PROTECTION PROFILE CONFORMANCE CLAIM

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

2.3 PACKAGE CLAIM

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

2.4 CONFORMANCE RATIONALE

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

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

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

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

Threat	Description
T.ACCOUNT	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.
T.CORRUPT	Corruption of data or loss of hardware may cause the loss of user data. Corruption or hardware loss may go undetected, resulting in even greater loss of user data.
T.UNDETECT	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed on the operational environment. Table 4 lists the OSP that is presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ENCRYPT	The TOE will provide a means to encrypt user data at rest.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

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

Assumptions	Description
A.ACCESS	The operational environment is responsible for protecting access to the management interfaces.
A.CRYPTO	Key management will be provided by the operational environment in support of data at rest encryption.
A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE. These administrators are not careless, wilfully negligent, or hostile, are appropriately trained and will follow the instructions provided by the TOE documentation.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

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

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

4.1 SECURITY OBJECTIVES FOR THE TOE

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

Security Objective	Description
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
O.ALERT	The TOE must be able to alert administrators to potential issues.
O.AUDIT	The TOE must record audit records for use of the TOE functions, and system health events. The TOE must provide a means to sort and review these records.
O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE.
O.PROTECT	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure. The TOE must protect audit data against unauthorized modification or removal.
O.PRIVATE	The TOE must ensure the confidentiality of user data by allowing the encryption of stored data.
O.TIME	The TOE must provide reliable timestamps.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

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

Security Objective	Description
OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
OE.KEY_MGMT	Key management will be provided by the operational environment in support of data at rest encryption.
OE.MGMT	The operational environment will protect access to the management interfaces.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.

Table 7 – Security Objectives for the Operational Environment

4.3 SECURITY OBJECTIVES RATIONALE

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

	T.ACCOUNT	T.CORRUPT	T.UNDETECT	P.ENCRYPT	A.ACCESS	A.CRYPTO	A.LOCATE	A.MANAGE
O.ACCESS	X							
O.ADMIN	X							
O.ALERT		X						
O.AUDIT			X					
O.IDENTAUTH	X							
O.PROTECT		X						

	T.ACCOUNT	T.CORRUPT	T.UNDETECT	P.ENCRYPT	A.ACCESS	A.CRYPTO	A.LOCATE	A.MANAGE
O.PRIVATE				X				
O.TIME			X					
OE.ADMIN								X
OE.KEY_MGMT						X		
OE.MGMT					X			
OE.PHYSICAL							X	

Table 8 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

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

Threat: **T.ACCOUNT**	An authorized user of the TOE could gain unauthorized access to TOE configuration information, or perform operations for which no access rights have been granted, via user error, system error, or other actions.	
Objectives:	O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data.
	O.ADMIN	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.
	O.IDENTAUTH	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against inadvertent access to administrative sessions by ensuring that sessions are closed when no longer in use.
Rationale:	O.ACCESS helps to mitigate the threat by restricting authorized users to only those TOE functions and data to which they have been granted access. O.ADMIN mitigates this threat by ensuring that access to the	

	security functions of the TOE are restricted to authorized users. O.IDENTAUTH helps to mitigate the threat by ensuring that only credentialed users have access to the TOE.	

Threat: **T.CORRUPT**	Corruption of data or loss of hardware may cause the loss of user data. Corruption or hardware loss may go undetected, resulting in even greater loss of user data.	
Objectives:	O.ALERT	The TOE must be able to alert administrators to potential issues.
	O.PROTECT	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure. The TOE must protect audit data against unauthorized modification or removal.
Rationale:	O.ALERT mitigates this threat by ensuring that administrators are alerted to potential issues. O.PROTECT mitigates this threat by protecting the availability and integrity of user data, and of the audit data that provides evidence of any irregularities.	

Threat: **T.UNDETECT**	Authorized or unauthorized users may be able to access TOE data or modify TOE behavior without a record of those actions in order to circumvent TOE security functionality.	
Objectives:	O.AUDIT	The TOE must record audit records for use of the TOE functions, and system health events. The TOE must provide a means to sort and review these records.
	O.TIME	The TOE must provide reliable timestamps.
Rationale:	O.AUDIT mitigates this threat by ensuring that audit entries record the use of TOE functions and system health events. O.TIME ensures that audit records are supported with accurate time information.	

4.3.2 Security Objectives Rationale Related to OSPs

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

Policy: **P.ENCRYPT**	The TOE will provide a means to encrypt user data at rest.	
Objectives:	O.PRIVATE	The TOE must ensure the confidentiality of

		user data by allowing the encryption of stored data.
Rationale:	O.PRIVATE supports this policy by ensuring that the TOE provides a means to encrypt stored data.	

4.3.3 Security Objectives Rationale Related to Assumptions

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

Assumption: A.ACCESS	The operational environment is responsible for protecting access to the management interfaces.	
Objectives:	OE.MGMT	The operational environment will protect access to the management interfaces.
Rationale:	OE.MGMT supports this assumption by ensuring that the operational environment protects access to the management interfaces.	

Assumption: A.CRYPTO	Key management will be provided by the operational environment in support of data at rest encryption.	
Objectives:	OE.KEY_MGMT	Key management will be provided by the operational environment in support of data at rest encryption.
Rationale:	OE.KEY_MGMT supports this assumption by ensuring the availability key management in support of data at rest encryption functions.	

Assumption: A.LOCATE	The TOE will be located within controlled access facilities, which will prevent unauthorized physical access.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
Rationale:	OE.PHYSICAL supports this assumption by protecting the TOE from physical attack.	

Assumption: A.MANAGE	There are one or more competent individuals assigned to manage the TOE.	
Objectives:	OE.ADMIN	There are an appropriate number of trusted, authorized administrators trained to administer the TOE. Authorized administrators are carefully selected and trained for proper operation of the TOE, follow all administrator guidance and are not malicious.
Rationale:	OE.ADMIN supports this assumption by ensuring that competent individuals are in place to manage the TOE and that those individuals have been specifically chosen to be careful, attentive and non-hostile, and are appropriately trained.	

5 EXTENDED COMPONENTS DEFINITION

5.1 SECURITY FUNCTIONAL REQUIREMENTS

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

a. Duplicate data removal (FDP_DDR _EXT.1)

5.1.1 Family FDP_DDR_EXT: Duplicate Data Removal

Duplicate data removal functions involve optimizing data storage by identifying segments of data that have already been stored and ensuring that redundancy is not caused by storing those segments multiple times for different data sets. The duplicate data removal family was modeled after FDP_SDI: Stored data integrity.

Family Behavior

This family defines the requirements for duplicate data removal functionality.

Component Levelling

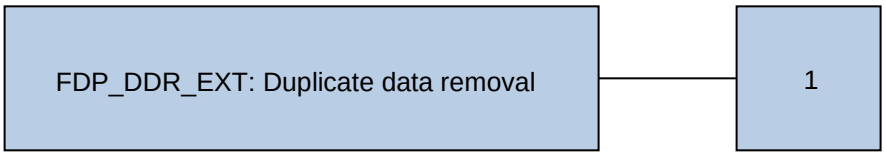

Figure 2 – FDP_DDR_EXT: Duplicate Data Removal Component Levelling

Management

There are no management activities foreseen.

Audit

There are no auditable events foreseen.

5.1.1.1 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [assignment: *action to be taken*] before writing new data to a storage container.

5.2 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

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

6.1 CONVENTIONS

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

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

6.2 SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 9.

Class	Identifier	Name
Security Audit (FAU)	FAU_ARP.1	Security alarms
	FAU_GEN.1	Audit data generation
	FAU_SAA.1	Potential violation analysis
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss

Class	Identifier	Name
Cryptographic Support (FCS)	FCS_COP.1	Cryptographic operation
User Data Protection (FDP)	FDP_DDR_EXT.1	Duplicate data removal
	FDP_SDI.2	Stored data integrity monitoring and action
Identification and Authentication (FIA)	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management (FMT)	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF (FPT)	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
Resource Utilization (FRU)	FRU_FLT.2	Limited fault tolerance
TOE Access (FTA)	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination

Table 9 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_ARP.1 Security alarms

Hierarchical to: No other components.

Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [*highlight new critical events in red and display them on the VxRail Manager dashboard*] upon detection of a potential security violation.

6.2.1.2 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) [*disk and node failures*].

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

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

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

6.2.1.3 FAU_SAA.1 Potential violation analysis

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [*one or more critical events*] known to indicate a potential security violation;

b) [*no other rules*].

6.2.1.4 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 [*authorised administrators*] with the capability to read [*event records*] from the audit records.

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

6.2.1.5 FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [*sorting*] of audit data based on [*ID number, severity or time*].

6.2.1.6 FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation

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

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

6.2.1.7 FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3 Action in case of possible audit data loss

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4.1 The TSF shall [overwrite the oldest stored audit records] and [*no other actions*] if the audit trail is full.

6.2.2 Cryptographic Support (FCS)

6.2.2.1 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 [*symmetric encryption*] in accordance with a specified cryptographic algorithm [*AES*[1]] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS*[2] *197*].

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_DDR_EXT.1 Duplicate data removal

Hierarchical to: No other components.

Dependencies: No dependencies

FDP_DDR_EXT.1.1 The TSF shall check incoming data to ensure that only unique data segments are stored in containers controlled by the TSF.

FDP_DDR_EXT.1.2 Upon detection of duplicate data, the TSF shall [*perform a global compression process and eliminate redundant data*] before writing new data to a storage container.

6.2.3.2 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: [*data checksums*].

FDP_SDI.2.2 Upon detection of a data integrity error, the TSF shall [*correct the error and create an alert*].

---

[1] Advanced Encryption Standard

[2] Federal Information Processing Standards

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

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

6.2.4.2 FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

Dependencies: FIA_UAU.1 Timing of authentication

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

6.2.4.3 FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1 Timing of identification

Dependencies: No dependencies.

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

6.2.5 Security Management (FMT)

6.2.5.1 FMT_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: [*configuration and monitoring of system/events, review of audit records*].

6.2.5.2 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 [*Hyper-Converged Infrastructure Administrator, VCenter Administrator, Linux Shell*].

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

6.2.6 Protection of the TSF (FPT)

6.2.6.1 FPT_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: [*disk or node failure*].

6.2.6.2 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 Resource Utilization (FRU)

6.2.7.1 FRU_FLT.2 Limited fault tolerance

Hierarchical to: FRU_FLT.1 Degraded fault tolerance

Dependencies: FPT_FLS.1 Failure with preservation of secure state

FRU_FLT.2.1 The TSF shall ensure the operation of all the TOE's capabilities when the following failures occur: [*disk or node failure*].

6.2.8 TOE Access (FTA)

6.2.8.1 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [*30 minutes of user inactivity*].

6.2.8.2 FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_SSL.4.1 The TSF shall allow user-initiated termination of the user's own interactive session.

6.3 SECURITY ASSURANCE REQUIREMENTS

The assurance requirements are summarized in Table 10.

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

Assurance Class	Assurance Components	
	Identifier	Name
Vulnerability Assessment (AVA)	AVA_VAN.2	Vulnerability analysis

Table 10 – Security Assurance Requirements

6.4 SECURITY REQUIREMENTS RATIONALE

6.4.1 Security Functional Requirements Rationale

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

	O.ADMIN	O.ALERT	O. AUDIT	O.IDENTAUTH	O.PROTECT	O.PRIVATE	O.TIME
FAU_ARP.1		x					
FAU_GEN.1			x				
FAU_SAA.1		x					
FAU_SAR.1			x				
FAU_SAR.3			x				
FAU_STG.1					x		
FAU_STG.4					x		
FCS_COP.1						x	
FDP_DDR_EXT.1					x		
FDP_SDI.2					x		
FIA_UAU.2				x			
FIA_UAU.7	x						
FIA_UID.2				x			
FMT_SMF.1	x						
FMT_SMR.1	x						
FPT_FLS.1					x		

	O.ADMIN	O.ALERT	O. AUDIT	O.IDENTAUTH	O.PROTECT	O.PRIVATE	O.TIME
FPT_STM.1							x
FRU_FLT.2					x		
FTA_SSL.3	x						
FTA_SSL.4	x						

Table 11 – Mapping of SFRs to Security Objectives

6.4.2 SFR Rationale Related to Security Objectives

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

Objective: **O.ADMIN**	The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.	
Security Functional Requirements:	FIA_UAU.7	Protected authentication feedback
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
	FTA_SSL.3	TSF-initiated termination
	FTA_SSL.4	User-initiated termination
Rationale:	FMT_SMF.1 provides the security management functions required to administer the security features of the TOE. FMT_SMR.1 provides roles that are used to restrict the use of security management functions. FIA_UAU.7 ensures that passwords are obscured as they are entered to prevent inadvertent access. FTA_SSL.4 ensures that users can close administrative sessions, and FTA_SSL.3 ensures that inactive administrative sessions are closed to prevent unauthorized use.	

Objective: **O.ALERT**	The TOE must be able to alert administrators to potential issues.	
Security Functional Requirements:	FAU_ARP.1	Security alarms
	FAU_SAA.1	Potential violation analysis
Rationale:	FAU_SAA.1 provides a means of identifying critical security issues, and FAU_ARP.1 ensures that these are brought to the administrator's attention.	

Objective: **O.AUDIT**	The TOE must record audit records for use of the TOE functions, and system health events. The TOE must provide a means to sort and review these records.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_SAR.1	Audit review
	FAU_SAR.3	Selectable audit review
Rationale:	FAU_GEN.1 ensures that audit records are generated for security relevant events. FAU_SAR.1 provides a means for administrators to review these records, and FAU_SAR.3 provides a means to sort audit records for ease of viewing.	

Objective: **O.IDENTAUTH**	The TOE must be able to identify and authenticate users prior to allowing access to the administrative functions and data of the TOE. The TOE must protect against inadvertent access to administrative sessions by ensuring that sessions are closed when no longer in use.	
Security Functional Requirements:	FIA_UAU.2	User authentication before any action
	FIA_UID.2	User identification before any action
Rationale:	FIA_UID.2 and FIA_UAU.2 ensures that administrative users are identified and authenticated before being granted access to TOE functions and data.	

Objective: **O.PROTECT**	The TOE must protect against the loss of TSF data and user data due to corruption or hardware failure. The TOE must protect audit data against unauthorized modification or removal.	
Security	FAU_STG.1	Protected audit trail storage

Functional Requirements:	FAU_STG.4	Prevention of audit data loss
	FDP_DDR_EXT.1	Duplicate data removal
	FDP_SDI.2	Stored data integrity monitoring and action
	FPT_FLS.1	Failure with preservation of secure state
	FRU_FLT.2	Limited fault tolerance
Rationale:	FDP_SDI.1 ensures that data is monitored for integrity errors, and corrected when correctable errors are detected. FDP_DDR_EXT.1 provides deduplication to remove extraneous data and make the integrity operations more efficient. FPT_FLS.1 ensures that a secure state is maintained in the case of disk or node failure. FRU_FLT.2 ensures that the TOE continues to operate in case of a disk or node failure. FAU_STG.1 ensures that audit data is protected from modification and unauthorized deletion. FAU_STG.4 ensures that audit data is handled in accordance with the policy in the case of a full audit trail	

Objective: **O.PRIVATE**	The TOE must ensure the confidentiality of user data by allowing the encryption of stored data.	
Security Functional Requirements:	FCS_COP.1	Cryptographic operation
Rationale:	FCS_COP.1 provides the encryption algorithm used to encrypt data a rest, thereby providing confidentiality of that data.	

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

6.4.3 Dependency Rationale

Table 12 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Dependency Satisfied	Rationale
FAU_ARP.1	FAU_SAA.1	✓	
FAU_GEN.1	FPT_STM.1	✓	
FAU_SAA.1	FAU_GEN.1	✓	
FAU_SAR.1	FAU_GEN.1	✓	
FAU_SAR.3	FAU_SAR.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FCS_COP.1	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1	✓	Satisfied by OE.KEY_MGMT in the operational environment
	FCS_CKM.4	✓	Satisfied by OE.KEY_MGMT in the operational environment
FDP_DDR_EXT.1	None	N/A	
FDP_SDI.2	None	N/A	
FIA_UAU.2	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FIA_UAU.7	FIA_UAU.1	✓	FIA_UAU.2 is hierarchical to FIA_UAU.1; this dependency has been satisfied.
FIA_UID.2	None	N/A	
FMT_SMF.1	None	N/A	
FMT_SMR.1	FIA_UID.1	✓	FIA_UID.2 is hierarchical to FIA_UID.1; this dependency has been satisfied.
FPT_FLS.1	None	N/A	
FPT_STM.1	None	N/A	
FRU_FLT.2	FPT_FLS.1	✓	
FTA_SSL.3	None	N/A	

SFR	Dependency	Dependency Satisfied	Rationale
FTA_SSL.4	None	N/A	

Table 12 – Functional Requirement Dependencies

6.4.4 Security Assurance Requirements Rationale

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

7 TOE SUMMARY SPECIFICATION

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

7.1 SECURITY AUDIT

7.1.1 Audit Generation and Review

VxRail generates audit records for administrative actions and health events, and stores them within the VxRail Manager. These logs are considered to be system events and can be viewed from the VxRail GUI on the Events page. These logs can be sorted by ID number, severity or time.

Records of system startup and shutdown, and Linux Shell access are recorded and stored within VxRail Manager under /var/log. These logs can only be viewed through the Linux Shell.

Log files can only be accessed through the VxRail application, and only authorized users are able to delete the log files. Logs are rotated once they reach a maximum size, except for the /var/log/audit.log file which is saved daily (or at maximum size of 11 MB), and the oldest file is removed when the folder reaches a total of 50MB. The maximum size for log files is as follows:

- /var/log/mystic files (except /var/log/mystic/hibernate and /var/log/mystic/management-account)
  - Maximum size is 50MB
- /var/log/mystic/hibernate.log
  - Maximum size is 50MB
- /var/log/mystic/management-account.log
  - Maximum size is 11MB
- /var/log/audit.log
  - Maximum size is 11 MB

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_SAR.1, FAU_SAR.3, FAU_STG.1, FAU_STG.4.

7.1.2 Security Alarms

VxRail Manager monitors the physical and logical system health. When a critical event is detected, the event is displayed on the VxRail Manager dashboard, highlighted in red. Once the event has been acknowledged, the red highlight is removed. Critical events include low storage capacity and failed hardware components.

TOE Security Functional Requirements addressed: FAU_ARP.1, FAU_SAA.1.

7.2 CRYPTOGRAPHIC SUPPORT

VxRail makes use of a cryptographic algorithm within vSAN to provide Data at Rest Encryption (D@RE). The symmetric algorithm is part of a FIPS 140-2

validated cryptographic module, CMVP certificate number 3073. Key management is provided by an external key manager.

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

TOE Security Functional Requirements addressed: FCS_COP.1.

7.3 USER DATA PROTECTION

7.3.1 Deduplication

Data deduplication optimizes the storage of user data by scanning all user data that is to be stored for segments of data that have already been stored (as part of a different set of user data). If a duplicate segment is found, the TOE will replace the duplicate segment with a pointer to the already-stored segment and store the rest of the unique user data.

The deduplication algorithm breaks the incoming data stream into segments and computes a unique fingerprint for the segment. This fingerprint is then compared to all others in the system to determine whether it is unique or redundant. Only unique data, and additional references to the previously stored unique segment, are stored to disk.

Deduplication is disabled by default. In the evaluated configuration, deduplication is enabled during the initial set up.

TOE Security Functional Requirements addressed: FDP_DDR_EXT.1.

7.3.2 Data Integrity

VxRail employs erasure coding and Redundant Array of Independent Disks (RAID) technology to detect and correct integrity errors. Erasure coding breaks up data into fragments and distributes redundant chunks of data across the system. It introduces redundancy by using data blocks and striping. Data blocks are grouped in sets of n, and for each set of n data blocks, a set of p parity blocks exists. Together, these sets of (n + p) blocks make up a stripe. Any of the n blocks in the (n + p) stripe is enough recover the entire data on the stripe.

As part of VxRail, vSAN implements Storage Policy Based Management, and each virtual machine deployed in a vSAN datastore has at least one assigned policy. When the VM is created and assigned a storage policy, the policy requirements are pushed to the vSAN layer. The storage policy indicates the number of host and device failures that a virtual machine object can tolerate. When erasure coding is enabled for a cluster, RAID 5 is applied if the number of Failures to tolerate is set to 1, and RAID 6 is applied if the number of Failures to tolerate is set to 2. Note that a vSAN cluster requires a minimum of four nodes for RAID 5 and six nodes for RAID 6.

In VxRail clusters, the data and parity blocks that belong to a single stripe are placed in different ESXi hosts in a cluster, providing a layer of failure tolerance for each stripe. Erasure coding provides single-parity data protection (RAID 5) that can tolerate one failure and double-parity data protection (RAID 6) that can

tolerate two failures. A single-parity stripe uses three data blocks and one parity block (3+1), and it requires a minimum of four hosts or four fault domains to ensure availability in case one of the hosts or disks fails. Dual parity uses four data blocks plus two parity blocks (4+2) and requires a minimum of six nodes.

When a hardware failure is detected, a critical event is indicated on the VxRail Manager dashboard to alert the administrator.

TOE Security Functional Requirements addressed: FDP_SDI.2.

7.4 IDENTIFICATION AND AUTHENTICATION

Authentication to the REST API, VxRail GUI and the Linux Shell is provided by the VCenter Single Sign On (SSO) component within VxRail. It prompts the user for a username and password and verifies that the user has a valid VCenter account. Users are assigned to user groups, and roles are assigned to the groups, such that all users within that group have the permissions associated with the assigned role. Administrative access is limited to users with the VCenter Administrator or Hyper-Converged Infrastructure Admin (HCIA) roles, which have the privileges required to log into VCenter.

Passwords are obscured as they are entered.

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

7.5 SECURITY MANAGEMENT

VxRail provides three management interfaces: VxRail GUI, REST API and Linux Shell.

- **VxRail GUI** - The VxRail GUI provides the security management functionality required to configure and administer the claimed security functionality. This interface is used to configure and monitor the hyper-converged infrastructure. Administrators can perform system configuration, view system events, and monitor logical and physical system health.
- **VxRail REST API** - The VxRail REST API provides a means of allowing organizations to customize management functionality.
- **Linux Shell** - The Linux Shell is used for maintenance requiring access to operating system level functions.

VxRail provides the following roles: Hyper-Converged Infrastructure Administrator, VCenter Administrator, and Linux Shell. The VxRail is preloaded with a user account, “Mystic”, which is assigned the Linux Shell role by default. The Linux Shell role cannot be assigned to any other user.

TOE Security Functional Requirements addressed: FMT_SMF.1, FMT_SMR.1.

7.6 PROTECTION OF THE TSF

vSAN and VxRail Appliances use fault domains to configure tolerance for rack and site failures. By default, a node is considered a fault domain. vSAN will spread components across fault domains, therefore, by default vSAN will spread components across nodes. For example, a cluster with four, four-node VxRail appliances, could have each appliance installed in a different rack. By explicitly defining each four-node appliance as separate fault domains, vSAN spreads redundancy components across the different racks. VxRail is capable of preserving a secure state with no loss of data in the case of full or partial loss of a node.

Timestamps are provided for use within VxRail, including the provision of timestamps for audit records. Time is synchronized with a Network Time Protocol (NTP) server to ensure consistency across the network.

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

7.7 RESOURCE UTILIZATION

In addition to preserving the secure state in the case of a disk or node failure, as described in Section 7.6, VxRail will also continue to operate in the case of disk or node failure resulting in the full or partial loss of a node.

TOE Security Functional Requirements addressed: FRU_FLT.1.

7.8 TOE ACCESS

Administrative users may log out of the GUI or the Linux Shell at any time. For the GUI only, the connection will timeout after 30 minutes of inactivity.

TOE Security Functional Requirements addressed: FTA_SSL.3, FTA_SSL.4.

8 ACRONYMS

8.1 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
D@RE	Data at Rest Encryption
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GUI	Graphical User Interface
HCIA	Hyper-Converged Infrastructure Admin
HDD	Hard Disk Drives
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
I/O	Input/Output
IT	Information Technology
NTP	Network Time Protocol
OSP	Organizational Security Policy
PaaS	Platform as a Service
PP	Protection Profile
PSC	Platform Services Controller
RAID	Redundant Array of Independent Disks
REST	Representational State Transfer
SDS	Software-Defined Storage
SFR	Security Functional Requirement

Acronym	Definition
SLES	SUSE Linux Enterprise Server
SSD	Solid State Drives
SSO	Single Sign On
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine
VSA	Virtual Storage Appliance

Table 13 – Acronyms