# Dell VxRail 7.0

# Security Target

**Evaluation Assurance Level (EAL): EAL2+**

**Version 1.0**

**February 2025**

**Document prepared by**


www.lightshipsec.com

# Document History

| Version | Date | Author | Description |
|---|---|---|---|
| 1.0 | 27 Feb 2025 | G. NICKEL | Release for certification |

# Table of Contents

**1 Introduction ..... 5**

1.1 Overview ..... 5
1.2 Identification ..... 5
1.3 Conformance Claims ..... 5
1.4 Terminology ..... 5

**2 TOE Description ..... 7**

2.1 Type ..... 7
2.2 Usage ..... 7
2.3 Logical Scope (Security Functions) ..... 9
2.4 Functionality Excluded from the Evaluated Configuration ..... 9
2.5 Physical Scope ..... 9
2.6 Guidance Documents ..... 11

**3 Security Problem Definition ..... 12**

3.1 Threats ..... 12
3.2 Assumptions ..... 12
3.3 Organizational Security Policies ..... 13

**4 Security Objectives ..... 13**

4.1 Objectives for the Operational Environment ..... 13
4.2 Objectives for the TOE ..... 13
4.3 Security Objectives Rationale ..... 14

**5 Extended Components Definition ..... 17**

5.1 Security Functional Requirements ..... 17
5.2 Security Assurance Requirements ..... 17

**6 Security Requirements ..... 18**

6.1 Conventions ..... 18
6.2 Security Functional Requirements ..... 18
6.3 Security Assurance Requirements ..... 25
6.4 Security Requirements Rationale ..... 26

**7 TOE Summary Specification ..... 30**

7.1 Security Audit ..... 30
7.2 Cryptographic Support ..... 30
7.3 User Data Protection ..... 31
7.4 Identification and Authentication ..... 31
7.5 Security Management ..... 31
7.6 Protection of the TSF ..... 32
7.7 Resource Utilization ..... 32
7.8 TOE Access ..... 32
7.9 Trusted Path ..... 32

# List of Tables

Table 1: Evaluation identifiers ..... 5
Table 2: Terminology ..... 5
Table 3: TOE Hardware and Software ..... 10
Table 4: Threats ..... 12
Table 5: Assumptions ..... 12
Table 6: Organizational Security Policies ..... 13

Table 7: Security Objectives for the Operational Environment ..... 13
Table 8: Security Objectives for the TOE ..... 14
Table 9: Security Objectives Rationale Mapping ..... 14
Table 10: Suitability of Security Objectives ..... 16
Table 11: Summary of SFRs ..... 18
Table 12: Assurance Requirements ..... 25
Table 13: Mapping of SFRs to Security Objectives ..... 26
Table 14: Suitability of SFRs ..... 26
Table 15: Dependency Rationale ..... 28

# 1 Introduction

## 1.1 Overview

1 This Security Target (ST) defines the Dell VxRail 7.0 Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 This document outlines 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.

## 1.2 Identification

**Table 1: Evaluation identifiers**

| | |
|---|---|
| **Target of Evaluation (TOE)** | Dell VxRail 7.0<br>Build: 7.0.533 |
| **Security Target (ST)** | Dell VxRail 7.0 Security Target, v1.0 |

## 1.3 Conformance Claims

3 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

4 This Security Target claims conformance to Evaluation Assurance Level 2 (EAL2) augmented with ALC_FLR.2 Flaw Reporting Procedures.

## 1.4 Terminology

**Table 2: Terminology**

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |

| Acronym | Definition |
|---|---|
| CAVP | Cryptographic Algorithm Validation Program |
| CC | Common Criteria |
| CLI | Command Line Interface |
| CM | Configuration Management |
| 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 |
| SLES | SUSE Linux Enterprise Server |
| SSD | Solid State Drives |
| SSO | Single Sign On |
| ST | Security Target |
| TLS | Transport Layer Security |
| TOE | Target of Evaluation |

| Acronym | Definition |
|---|---|
| TSF | TOE Security Functionality |
| VM | Virtual Machine |
| VSA | Virtual Storage Appliance |

# 2 TOE Description

## 2.1 Type

5 The TOE is a hyper-converged appliance (other devices and systems)

## 2.2 Usage

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

7 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.

8 VxRail provides the following storage, virtualization and security functionality:

### 2.2.1 Storage

9 VMware vSAN 7.0 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 7.0 kernel's Input/Output (I/O) data path. vSAN pools the VxRail Appliance's installed storage disks (see Table 3 for drive capacity information) 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.

### 2.2.2 Virtualization

10 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.

### 2.2.3 Security

11 VxRail provides the following security functionality:

a) Security audit generation, review and secure storage of audit records

b) Monitoring of system health

c) Encryption of data at rest

d) Assurance of data deduplication

e) Identification and authentication of administrative users

f) Secure management through VxRail Manager

g) Timeout of inactive administrative sessions

12 The TOE is a combined software and hardware TOE as depicted in Figure 1 below.

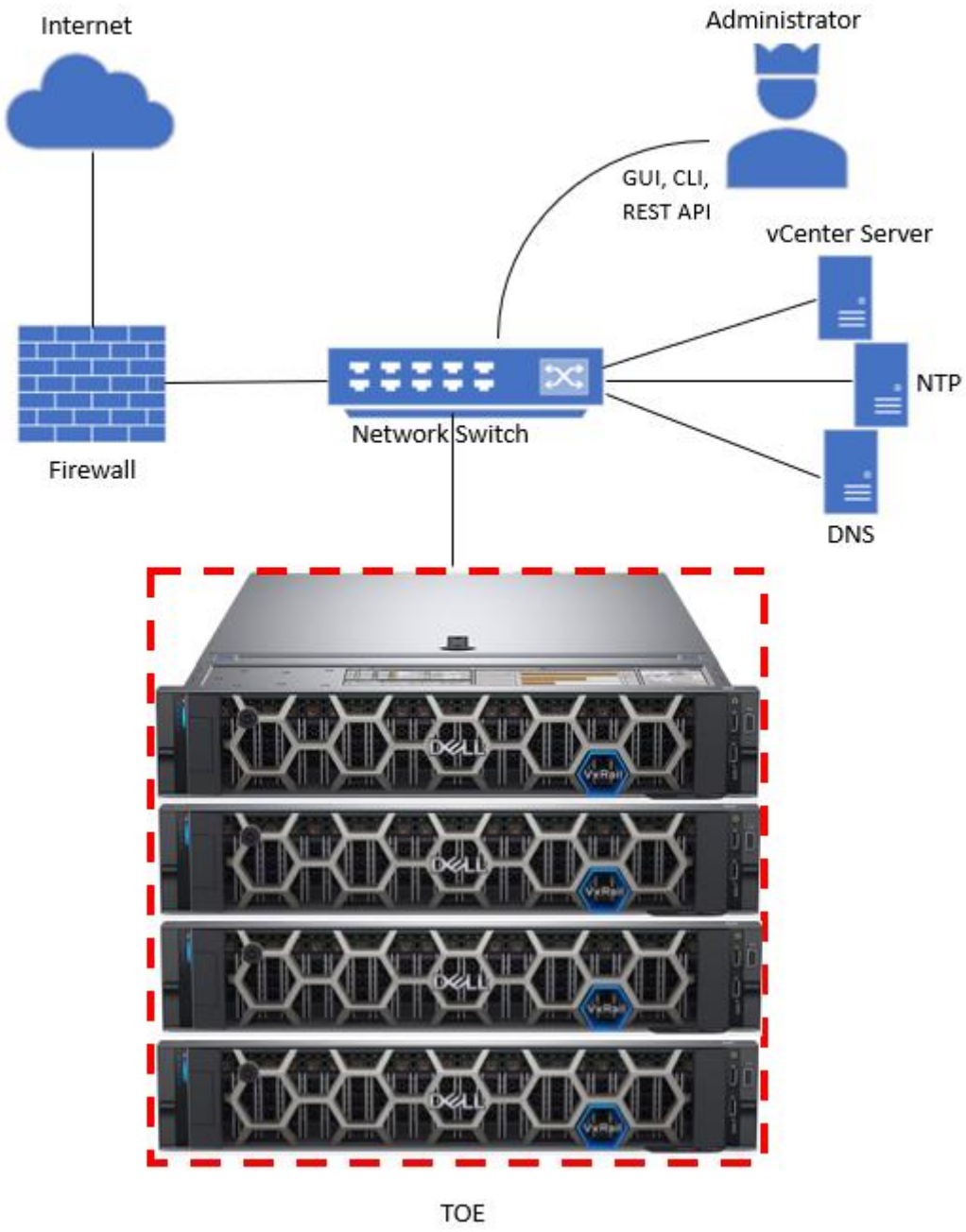


**Figure 1: TOE Boundary**

## 2.3 Logical Scope (Security Functions)

13 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 below. The TOE provides the following security functions:

a) **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.

b) **Cryptographic Support.** Cryptographic functionality is provided to protect the confidentiality of user data at rest.

c) **User Data Protection.** Duplicate data is removed before it is written to storage for protection against redundant storage utilization.

d) **Identification and Authentication.** Users must identify and authenticate prior to TOE access. Passwords are obscured as they are entered.

e) **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 remotely via Hypertext Transfer Protocol Secure (HTTPS), and a Command Line Interface (CLI) accessed remotely via SSHv2. Management functions allow the administrators to manage system health and review audit records.

f) **Protection of the TSF.** A secure state is maintained in the case of disk or node failure. Reliable timestamps are provided for audit records.

g) **Resource Utilization**. The TOE ensures continued operation in the case of disk or node failure.

h) **TOE Access**. Administrative users may log out of an interactive session at any time. Inactive sessions are closed after 30 minutes of inactivity.

## 2.4 Functionality Excluded from the Evaluated Configuration

### 2.4.1 Excluded Services

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

- SRS VE
- VMCloudware VCF

### 2.4.2 Excluded Interfaces

15 In the evaluated configuration, the TOE 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.

## 2.5 Physical Scope

16 The TOE is the VxRail appliance running VxRail Manager 7.0 software. The deployment configuration and TOE boundary are shown in Figure 1.

17 The physical boundary of the TOE is limited to the hardware and software listed in Table 3.

**Table 3: TOE Hardware and Software**

| Model | Manufacturer | Processor | Memory Capacity | Drive Capacity | Software/OS |
|---|---|---|---|---|---|
| E660F (15G) Appliance | Dell | Intel Xeon Silver (Ice Lake)<br>Intel Xeon Gold (Ice Lake)<br>Intel Xeon Platinum (Ice Lake) | 64 GB to 8192 GB | 10 x 2.5” drive bays (SAS/SATA)<br>Or<br>8 x 2.5” drive bays (SAS/SATA)<br>2 x 2.5” drive bays (NVMe) | VxRail Manager 7.0 |
| P670F (15G) Appliance | Dell | Intel Xeon Silver (Ice Lake)<br>Intel Xeon Gold (Ice Lake)<br>Intel Xeon Platinum (Ice Lake) | 64 GB to 4096 GB | 24 x 2.5” drive bays (all Flash or all NVMe) | |
| P670N (15G) Appliance | Dell | Intel Xeon Silver (Ice Lake)<br>Intel Xeon Gold (Ice Lake)<br>Intel Xeon Platinum (Ice Lake) | 64 GB to 4096 GB | 10 x 2.5” drive bays (all NVMe) | |
| S670 (15G) Appliance | Dell | Intel Xeon Silver (Ice Lake)<br>Intel Xeon Gold (Ice Lake)<br>Intel Xeon Platinum (Ice Lake) | 64 GB to 4096 GB | 12 x 3.5” front drive bays<br>4 x 2.5” rear drive bays (Hybrid) | |
| V670F (15G) Appliance | Dell | Intel Xeon Silver (Ice Lake)<br>Intel Xeon Gold | 128 GB to 4096 GB | 24 x 2.5” drive bays (all Flash) | |

| Model | Manufacturer | Processor | Memory Capacity | Drive Capacity | Software/OS |
|---|---|---|---|---|---|
| | | (Ice Lake)<br><br>Intel Xeon Platinum (Ice Lake) | | | |

18 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 Professional Services team.

### 2.5.1 Non-TOE Components

19 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 |
| Network Time Protocol (NTP) Service | N/A | N/A |
| vCenter Server | VMware PhotonOS | General Purpose Server Hardware |
| Key Management Server | VMware Native Key Provider (NKP) | General Purpose Server Hardware |
| DNS Server | Windows Server | General Purpose Server Hardware |

## 2.6 Guidance Documents

20 The TOE includes the following guidance documentation. The documents may be downloaded in PDF format from the Dell support website here: https://www.dell.com/support/home/en-ca/product-support/product/vxrail-software/docs

a) Dell VxRail™ 7.0 Administration Guide, Rev. 22, September 2024

b) Dell VxRail™ Security Configuration Guide, Rev. 13, January 2025

c) Dell VxRail™ API User Guide for 4.5.x, 4.7.x, and 7.0.x, Rev. 22, February 2022

d) Dell VxRail™ 7.0 Common Criteria Guide, Version 1.0, February 2025

# 3 Security Problem Definition

## 3.1 Threats

21 Table 4 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 willfully 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.

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

**Table 4: Threats**

| 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 | User data could become corrupt or otherwise inaccessible due to hardware failure or invalid system access by TOE users or attackers. |
| 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. |

## 3.2 Assumptions

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

**Table 5: Assumptions**

| Assumption | 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. |

## 3.3 Organizational Security Policies

24 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.

**Table 6: Organizational Security Policies**

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

# 4 Security Objectives

25 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 operational environment
- Security objectives for the TOE

## 4.1 Objectives for the Operational Environment

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

**Table 7: Security Objectives for the Operational Environment**

| 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. |

## 4.2 Objectives for the TOE

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

**Table 8: Security Objectives for 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, via secure channels, 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. |

## 4.3 Security Objectives Rationale

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

**Table 9: Security Objectives Rationale Mapping**

| | 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 | | | | | |

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

29 Table 10 provides the justification to show that the security objectives are suitable to address the security problem and map back to the threats, assumptions, and OSP's.

**Table 10: Suitability of Security Objectives**

| Element | Justification |
|---|---|
| **Threats** | |
| T.ACCOUNT | **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.<br>**O.ADMIN** mitigates this threat by ensuring that access to the<br>security functions of the TOE are restricted to authorized users.<br>**O.IDENTAUTH** helps to mitigate the threat by ensuring that the TOE is able to identify and authenticate users prior to allowing access to the administrative functions of the TOE. |
| T.CORRUPT | **O.ALERT** mitigates this threat by ensuring that administrators are alerted to potential issues.<br>**O.PROTECT** mitigates this threat by protecting the availability of user data, and of the audit data that provides evidence of any irregularities. |
| T.UNDETECT | **O.AUDIT** mitigates this threat by ensuring that audit entries record the use of TOE functions and system health events.<br>**O.TIME** ensures that audit records are supported with accurate time information. |
| **Assumptions** | |
| A.ACCESS | **OE.MGMT** supports this assumption by ensuring that the operational environment protects access to the management interfaces. |
| A.CRYPTO | **OE.KEY_MGMT** supports this assumption by ensuring the availability key management in support of data at rest encryption functions. |
| A.LOCATE | **OE.PHYSICAL** supports this assumption by protecting the TOE from physical attack. |
| A.MANAGE | **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. |
| **Organizational Security Policies** | |
| P.ENCRYPT | **O.PRIVATE** supports this policy by ensuring that the TOE provides a means to encrypt stored data. |

# 5 Extended Components Definition

## 5.1 Security Functional Requirements

30 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**

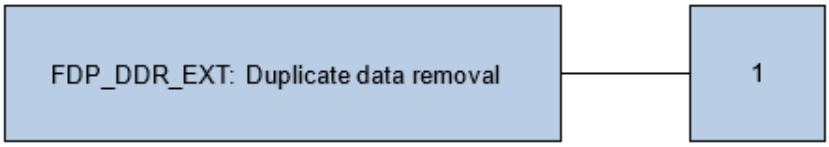


**Figure 2: FDP_DDR_EXT: Duplicate Data Removal Component Levelling**

**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

31 This ST does not include extended Security Assurance Requirements.

# 6 Security Requirements

32 This section 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

33 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

34 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 11.

**Table 11: Summary of SFRs**

| 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 |
| Cryptographic Support (FCS) | FCS_COP.1 | Cryptographic operation |
| User Data Protection (FDP) | FDP_DDR_EXT.1 | Duplicate data removal |
| Identification and Authentication (FIA) | FIA_UAU.1 | Timing of Authentication |
| | FIA_UAU.2 | User authentication before any action |
| | FIA_UAU.7 | Protected authentication feedback |
| | FIA_UID.1 | Timing of Identification |

| Class | Identifier | Name |
|---|---|---|
| | 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 |
| Trusted Path/Channel (FTP) | FTP_TRP.1 | Trusted Path |

## 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*] and cryptographic key sizes [*256 bits*] that meet the following: [*FIPS 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.

## 6.2.4 Identification and Authentication (FIA)

### 6.2.4.1 FIA_UAU.1 Timing of Authentication

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

**FIA_UAU.1.1** The TSF shall allow [*no TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

**FIA_UAU.1.2** 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.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.

#### 6.2.4.3 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.

#### 6.2.4.4 FIA_UID.1 Timing of Identification

Hierarchical to: No other components.

Dependencies: No dependencies

**FIA_UID.1.1** The TSF shall allow [*no TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

**FIA_UID.1.2** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

#### 6.2.4.5 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.

## 6.2.9 Trusted Path/Channels (FTP)

### 6.2.9.1 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 [*remote administration*].

## 6.3 Security Assurance Requirements

35 The TOE security assurance requirements are summarized in Table 12 commensurate with EAL2+ (ALC_FLR.1).

**Table 12: Assurance Requirements**

| Assurance Class | Components | Description |
|---|---|---|
| ADV: Development | ADV_ARC.1 | Security Architecture Description |
| | ADV_FSP.2 | Security-enforcing Functional Specification |
| | ADV_TDS.1 | Basic Design |
| AGD: Guidance Documents | AGD_OPE.1 | Operational User Guidance |
| | AGD_PRE.1 | Preparative Procedures |
| ALC: Life Cycle Support | 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 |
| 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 |
| ATE: Tests | ATE_COV.1 | Evidence of Coverage |
| | ATE_FUN.1 | Functional testing |
| | ATE_IND.2 | Independent Testing – sample |
| AVA: Vulnerability Assessment | AVA_VAN.2 | Vulnerability Analysis |

## 6.4 Security Requirements Rationale

### 6.4.1 Security Functional Requirements Rationale

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

**Table 13: Mapping of SFRs to Security Objectives**

| | O.ACCESS | 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 | | |
| FIA_UAU.1 | x | | | | x | | | |
| FIA_UAU.2 | x | | | | x | | | |
| FIA_UAU.7 | | x | | | | | | |
| FIA_UID.1 | x | | | | x | | | |
| FIA_UID.2 | x | | | | x | | | |
| FMT_SMF.1 | x | x | | | | | | |
| FMT_SMR.1 | x | x | | | | | | |
| FPT_FLS.1 | | | | | | x | | |
| FPT_STM.1 | | | | | | | | x |
| FRU_FLT.2 | | | | | | x | | |
| FTA_SSL.3 | | x | | | | | | |
| FTA_SSL.4 | | x | | | | | | |
| FTP_TRP.1 | | x | | | | | | |

### 6.4.2 SFR Rationale Related to Security Objectives

37 Table 14 provides rationale for the suitability of each SFR to the mapped Security Objectives for the TOE.

38 Table 15 provides the dependency rationale for each SFR claimed.

**Table 14: Suitability of SFRs**

| Element | Justification |
|---|---|
| O.ACCESS | **FIA_UID.1, FIA_UID.2, FIA_UAU.1, and FIA_UAU.2**. Ensures that administrative users are identified and authenticated before being granted access to TOE functions and data.<br>**FMT_SMF.1.** provides the security management functions required to administer the security features of the TOE.<br>**FMT_SMR.1.** provides roles that are used to restrict the use of security management functions. |
| O.ADMIN | **FIA_UAU.7.** Ensures that passwords are obscured as they are entered to prevent inadvertent access.<br>**FMT_SMF.1.** provides the security management functions required to administer the security features of the TOE.<br>**FMT_SMR.1.** provides roles that are used to restrict the use of security management functions.<br>**FTA_SSL.3.** Ensures that inactive administrative sessions are closed to prevent unauthorized use<br>**FTA_SSL.4.** Ensures that users can close administrative sessions<br>**FTP_TRP.1.** Ensures that encrypted channels are used for remote administration. |
| O.ALERT | **FAU_ARP.1.** Ensures that these are brought to the administrator's attention.<br>**FAU_SAA.1.** Provides a means of identifying critical security issues |
| O.AUDIT | **FAU_GEN.1.** Ensures that audit records are generated for security relevant events.<br>**FAU_SAR.1.** Provides a means for administrators to review these records<br>**FAU_SAR.3**. Provides a means to sort audit records for ease of viewing. |
| O.IDENTAUTH | **FIA_UID.1, FIA_UID.2, FIA_UAU.1, and FIA_UAU.2**. Ensures that administrative users are identified and authenticated before being granted access to TOE functions and data. |
| O.PROTECT | **FAU_STG.1**. Ensures that audit data is protected from modification and unauthorized deletion.<br>**FAU_STG.4**. Ensures that audit data is handled in accordance with the policy in the case of a full audit trail<br>**FDP_DDR_EXT.1.** Provides deduplication to remove extraneous data.<br>**FPT_FLS.1.** Ensures that a secure state is maintained in the case of disk or node failure.<br>**FRU_FLT.2.** Ensures that the TOE continues to operate in case of a disk or node failure. |
| O.PRIVATE | **FCS_COP.1.** Provides the encryption algorithm used to encrypt data a rest, thereby providing confidentiality of that data. |
| O.TIME | **FPT_STM.1.** Ensures the provision of reliable time stamps. |

**Table 15: Dependency Rationale**

| SFR | Dependency | Rationale |
|---|---|---|
| FAU_ARP.1 | FAU_SAA.1 | Met |
| FAU_GEN.1 | FPT_STM.1 | Met |
| FAU_SAA.1 | FAU_GEN.1 | Met |
| FAU_SAR.1 | FAU_GEN.1 | Met |
| FAU_SAR.3 | FAU_SAR.1 | Met |
| FAU_STG.1 | FAU_GEN.1 | Met |
| FAU_STG.4 | FAU_STG.1 | Met |
| FCS_COP.1 | FDP_ITC.1 | Not met.<br>(Not required per CCCS policy) |
| | FDP_ITC.2 | |
| | FCS_CKM.1 | |
| | FCS_CKM.4 | |
| FDP_DDR_EXT.1 | None | - |
| FIA_UAU.1 | FIA_UID.1 | Met |
| FIA_UAU.2 | FIA_UID.1 | Met |
| FIA_UAU.7 | FIA_UAU.1 | Met |
| FIA_UID.1 | None | - |
| FIA_UID.2 | None | - |
| FMT_SMF.1 | None | - |
| FMT_SMR.1 | FIA_UID.1 | Met |
| FPT_FLS.1 | None | - |
| FPT_STM.1 | None | - |
| FRU_FLT.2 | FPT_FLS.1 | Met |
| FTA_SSL.3 | None | - |
| FTA_SSL.4 | None | - |

| SFR | Dependency | Rationale |
|---|---|---|
| FTP_TRP.1 | None | - |

### 6.4.3 Security Assurance Requirements Rationale

39 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

40 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

41 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.

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

43 Log files can only be accessed through VxRail Manager, 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/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/management-account)
  - i) Maximum size is 50MB
- /var/log/mystic/management-account.log
  - i) Maximum size is 10MB
- /var/log/audit/audit.log
  - i) Maximum size is 11MB

44 **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

45 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.

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

## 7.2 Cryptographic Support

47 VxRail makes use of the underlying VMWare environment for vSAN to provide the AES-256 cryptographic algorithm for Data-at-Rest Encryption (D@RE) functions. This symmetric algorithm is provided by a FIPS 140-2 validated cryptographic module within the VMware vSAN software (VMware VMkernel Cryptographic Module) CAVP cert #C1172. FCS_COP.1 has been claimed in support of this functionality.

48 **TOE Security Functional Requirements addressed:** FCS_COP.1.

## 7.3 User Data Protection

### 7.3.1 Deduplication

49 Data deduplication is provided by the vSAN software and is designed to optimize 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 leverage vSAN to replace the duplicate segment with a pointer to the already-stored segment and store the rest of the unique user data.

50 The deduplication algorithm implemented by vSAN breaks the incoming data stream into segments and computes a unique fingerprint consisting of a SHA-1 hash value for the segment. This fingerprint is then compared to all others in the system to determine whether it is unique or redundant. Hash values used for the fingerprints are stored on disk in a vSAN specific hash-map. Only unique data, and additional references to the previously stored unique segment, are written to disk.

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

52 **TOE Security Functional Requirements addressed:** FDP_DDR_EXT.1.

## 7.4 Identification and Authentication

53 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.

54 Passwords are obscured as they are entered.

55 **TOE Security Functional Requirements addressed:** FIA_UAU.1, FIA_UAU.2, FIA_UAU.7, FIA_UID.1, FIA_UID.2.

## 7.5 Security Management

56 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.

57 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.

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

## 7.6 Protection of the TSF

59 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.

60 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.

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

## 7.7 Resource Utilization

62 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.

63 **TOE Security Functional Requirements addressed:** FRU_FLT.1.

## 7.8 TOE Access

64 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.

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

## 7.9 Trusted Path

66 For all management interfaces (Web GUI, CLI, REST API) the OpenSSL FIPS library is leveraged by the TOE to implement secure HTTPS/TLS and SSH communications via known-good implementation.

67 All communications between remote administrators and the Web GUI interface are protected using TLS v1.2 with ECDHE curves: prime256v1, secp384r1, secp521r1 and the following ciphersuites:.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

68 All communications using the REST API interface are protected using TLS v1.2 and TLS v1.3 with P-384 curves and support the following ciphersuites:

TLS v1.2

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

TLS v1.3

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384

69 Communications with remote administrators via the CLI interface is protected by using SSHv2 with password-based authentication. The following SSH characteristics are supported in the evaluated configuration:

a) Encryption Algorithms
   - aes256-ctr
   - aes256-gcm@openssh.com

b) MAC Algorithms
   - hmac-sha2-256
   - hmac-sha2-512

c) Key Exchange Algorithms
   - ecdh-sha2-nistp384

d) Host Keys
   - rsa-sha2-512
   - ecdsa-sha2-nistp256

70 **TOE Security Functional Requirements addressed:** FTP_TRP.1.