Nutanix, Inc.

Nutanix Cloud Platform

v6.8

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.16

Prepared for:

Nutanix, Inc.
1740 Technology Drive
Suite 150
San Jose, CA, 95110
United States of America

Phone: +1 855 688 2649
www.nutanix.com

Prepared by:

Corsec Security, Inc.
12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is comprised of:

- Acropolis Operating System (AOS) v6.8
- Acropolis Hypervisor (AHV) v20230302.100173
- Prism Central (PC) pc.2024.2.0.6
- Flow Virtual Networking (FVN) v4.0.0
- Flow Network Security (FNS) v4.1.0
- Self-Service v3.8.1.1
- Files v5.0.0.1
- Objects v5.0
- Nutanix Database (NDB) v2.5.5

These are collectively referred to as the Nutanix Cloud Platform or NCP and will hereafter be referred to as the TOE throughout this document. A minimum of three hosts (either nodes or servers) that contain a copy of the TOE are combined to provide a High Availability (HA) cluster. This allows the TOE to be a unified solution for guest Virtual Machine (VM) management while eliminating administration overhead by removing the need for a separate storage network.

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3. There are no extended SARs defined for this ST.
- Security Requirements (Section 6) – Presents the SFRs and SARs to which the TOE adheres.
- TOE Summary Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.

- Rationale (Section 8) - Presents the rationale for the security objectives, requirements, and SFR dependencies as to their consistency, completeness, and suitability.
- Acronyms (Section 9) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 below shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Nutanix, Inc. Nutanix Cloud Platform v6.8 Security Target*
ST Version	Version 0.16
ST Author	Corsec Security, Inc.
ST Publication Date	11/02/2026
TOE Reference	Nutanix Cloud Platform v6.8

1.3 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. This section provides a context for the TOE evaluation by identifying the TOE type, describing the TOE, and defining the specific evaluated configuration.

The TOE is software that provides a secure, resilient, and self-healing platform for building a hybrid multi-cloud infrastructure to support all kinds of workloads and use cases across public and private clouds, multiple hypervisors and containers, with varied compute, storage, and network requirements.

The TOE consists of all the Nutanix software that makes-up Nutanix Cloud Platform, in a three-node cluster. The host appliance is considered to be within the TOE environment. Nutanix Cloud Platform v6.8 consists of the following software components:

- Acropolis Operating System (AOS) v6.8
- Acropolis Hypervisor (AHV) v20230302.100173
- Prism Central (PC) pc.2024.2.0.6
- Flow Virtual Networking (FVN) v4.0.0
- Flow Network Security (FNS) v4.1.0
- Self-Service v3.8.1.1
- Files v5.0.0.1
- Objects v5.0
- Nutanix Database (NDB) v2.5.5

The TOE offers two web Graphical User Interfaces (GUIs), called Prism Element and Prism Central respectively. The TOE also offers management of various services via REST API v2, v3, and v4. Finally, the Nutanix Database Service (NDB) leverages a GUI, CLI, and REST API specific to NDB, referred to as the NDB GUI, NDB CLI, and NDB REST API respectively.

Nutanix Cloud Platform provides the capabilities to run guest VMs in the operating environment via the CVM hosted by AHV. The guest VMs run services that make use of the storage provided by and managed by the CVM. Guest VMs can be imported to the product from any supported CVM such as VMware ESXi, KVM[1], or Hyper-V. Administrative users can backup guest VM data along with user data through replication functionality available through Nutanix Cloud Platform.

The TOE enforces a Virtual Disk Access Security Functionality Policy (SFP) on guest VMs that the TOE hosts. This SFP controls guest VM access to the storage that the TOE provides. In order to determine if a guest VM can access a virtual disk, the TOE first checks an NFS whitelist and then checks if the guest VM has been configured to access the NFS share.

The TOE enforces a Virtual Disk Locking SFP on clients attempting to write to or execute files stored on virtual disks. This SFP allows a read or execute operation if the process requesting the operation has obtained a virtual disk lock. If a virtual disk lock does not currently exist for the virtual disk, the TOE allows the process to obtain a virtual disk lock. Otherwise, the operation request is denied.

The TOE generates audit records for all configuration changes made via the management interfaces. Within these audit records, the TOE includes basic information about the event in a human-readable format. The TOE environment is responsible for providing the reliable timestamps according to the A.TIME assumption.

The TOE includes a set of management interfaces that administrative users can use to view the audit logs, configure failover functionality, manage TOE settings, manage accounts, and configure the storage provided by the TOE. The management interfaces can also be used to configure the Virtual Disk Access SFP and Virtual Disk Locking SFPs. Storage options include access type (pass-through or virtual disk format), tiering options (PCIe SSD, SSD, or HDD), and maximum capacity allocated. There are seven administrative roles defined for the TOE, enforced by the Role Based Access Control (RBAC) SFP: Super Admin, Prism Admin, and Prism Viewer. Administrative users can log out of their management sessions at any time.

The TOE requires administrative users to perform identification and authentication before accessing any TOE functionality.

1.4 TOE Environment

The TOE environment contains the hardware of three hosts and can optionally contain additional hosts with their own instances of the TOE to provide increased redundancy and scalability. The TOE is capable of running on any of the Nutanix appliance hardware platforms listed in Appendix A – Supported Hardware Platforms – in the evaluated configuration, the three-node NX-3060-G8 is used. The network infrastructure that provides connectivity between all entities is also part of the TOE environment.

The TOE is designed to run and store multiple guests VMs that in turn offer services to end users, and are considered to be environmental components running on the TOE. At least one guest VM must be running in order to make use of the storage functionality provided by the TOE.

A management workstation is required to access the TOE's management interfaces. No minimum requirements are enforced.

Administrative users should access Prism Element, Prism Central, and NDB GUI through the latest version of a web browser such as:

- Mozilla Firefox
- Google Chrome

[1] KVM – Kernel-based Virtual Machine

- Apple Safari
- Microsoft Edge
- Microsoft Internet Explorer 11

The REST API interfaces may be accessed using any REST API client, such as Postman.

It is assumed that only trusted users or software have access to the host hardware components. In addition, the host hardware components are intended to be deployed in a physically secure cabinet, room, or data center with the appropriate level of physical access control and physical protection (e.g. badge access, fire control, locks, alarms, etc.).

The TOE must have access to an NTP server that can provide reliable time stamps to the TOE.

1.5 TOE Description

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

1.5.1 Physical Scope

The physical scope of the TOE includes the 9 components identified in section 1.3. AHV provides the basic interface to the host hardware and provides a virtualized space for AOS to run within a CVM. AOS provides all of the non-virtualization functionality for the TOE.

The evaluated configuration of the TOE was tested on the three-node NX-3060N-G8 (also referred to as the NX-3360N-G8, where the "3" in the place of the “0” denotes the three nodes of the platform) hardware platform running Nutanix Cloud Platform v6.8. NCP was not tested on, but is capable of running on other host hardware and is derived from a single monolithic image, which detects the hardware platform specifications and enables the appropriate drivers to support the host’s hardware. The following host hardware each support at least 8 CPU cores and 128GB of memory, and can be used with the TOE software:

- NX-1065-G8
- NX-1065-G9
- NX-1065N-G8
- NX-1175S-G8
- NX-1175S-G9
- NX-3035-G9
- NX-3060-G8
- NX-3060-G9
- NX-3155G-G8
- NX-3155GN-G8
- NX-3155-G9
- NX-3170-G8
- NX-3170N-G8
- NX-8035-G8
- NX-8035N-G8
- NX-8150-G8
- NX-8150-G9
- NX-8150N-G8
- NX-8155-G8
- NX-8155N-G8
- NX-8155-G9
- NX-8155A-G9
- NX-8170-G8
- NX-8170N-G8
- NX-8170-G9

Hardware platforms listed with a “1” in the second numerical position (ex. NX-8170N-G8) are available only as single-node platforms. Single-node platforms are intended to scale out infrastructure and provide an additional node to an existing cluster.

Platforms with a “0” in the second numerical position (ex. NX-1065-G8) are available in 2, 3, and 4-node configurations, in which case the “0” in the model number may be replaced by the number of nodes in the system (ex. A 4-node NX-1065-G8 may also be referred to as the NX-1465-G8).

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE.

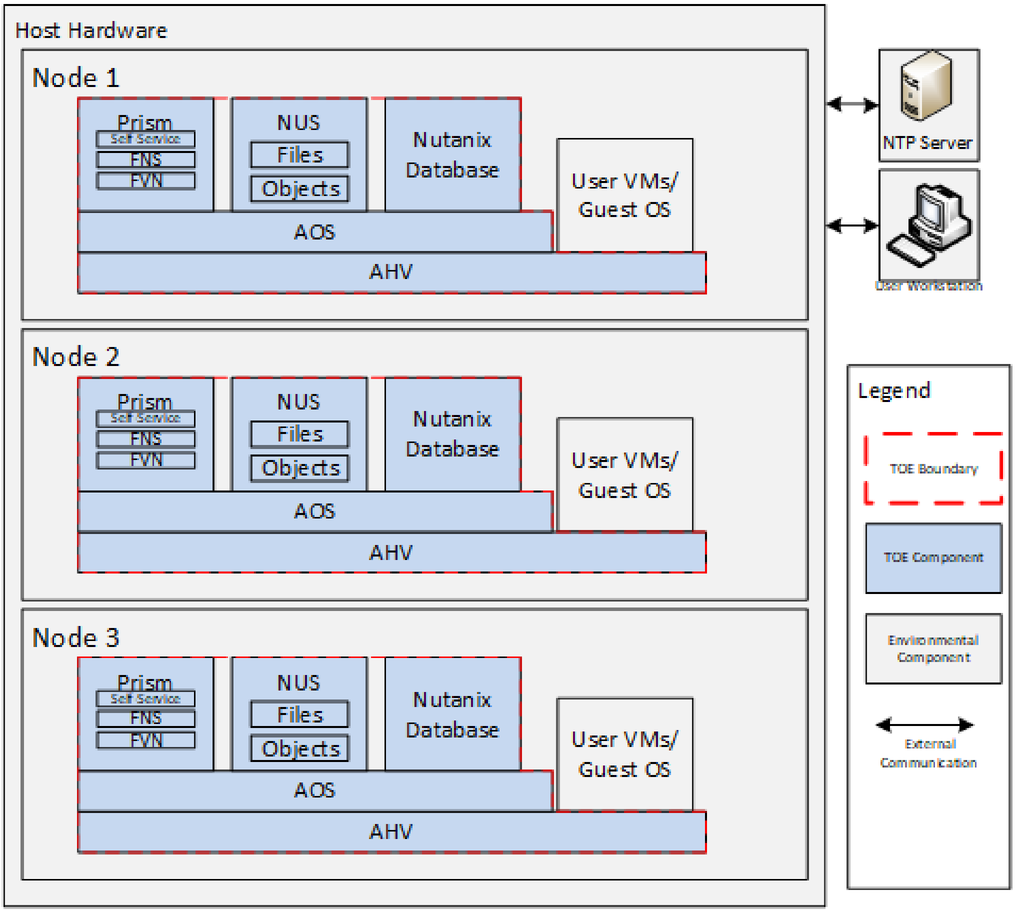

Figure 1 – Physical TOE Boundary

The TOE boundary includes:

- the Nutanix-developed AOS and AHV of the three-node deployment for NCP
- the Nutanix software components running on AOS
- Nutanix-modified third-party source code or software

The TOE boundary does not include the following environmental components shown in Figure 1:

- Guest VMs running on AHV
- Workstations
- Host hardware, chassis, or disks
- NTP server

The following is not depicted in the diagram and is considered to be part of the TOE environment:

- Web browser running on the user workstation

At least one guest VM must be running as part of the TOE environment in order for the storage functionality provided by the TOE to be used.

1.5.1.1 TOE Software/Hardware

The TOE is a software-only TOE which comes pre-installed on certified Nutanix hardware. Software images for the TOE can be downloaded from the Nutanix Support Portal at http://portal.nutanix.com/ for re-imaging and upgrading the TOE software version. Different software images may be used depending on whether the user is re-imaging or upgrading the TOE software. Only a registered user may access and download the software images.

The software images for each component are packaged as follows:

Table 2 – TOE Component Software

Component	Filename	Hash
AHV	**ISO:** AHV-DVD-x86_64-el8.nutanix.20230302.100173.iso	**SHA256:**05f392a5e02ddcac9b84d010715f4d2d993b87b1430643e09524295e3a8282ff
	LCM[2]: lcm_ahv_el8.nutanix.20230302.100173.tar.gz	**SHA256:**0e41e56a772570c5bc50a4db393c479e7787cfa51fb5e52495813cfaff5f1315
AOS	**Upgrade:** nutanix_installer_package-release-fraser-6.8-stable-9b27c8bcb5fcaac58016f3bed74009655a157049-x86_64.tar.gz	**SHA256:**f8192c654ac45a714dc56d0532595c9dfa18bdc9183122d53b79b1daefa242db
	LCM: lcm_nos_6.8.tar.gz	**SHA256:**b7b850d5fb8e90399b464b3422cb562720e686195cd4a37c8edb977b4714fa36
Prism Central	**Upgrade:** pc.2024.2.0.6-e7141238ee6a3838cb87a1467496b119224bb219-x86_64.tar.gz	**SHA256:** b2731240c1d33b071c08b3d2699367cd71f8d7ab1610e1c4bf5036c22bb2edc1
	LCM: lcm_pc_pc.2024.2.0.6.tar.gz	**SHA256:** bac961593477e6dcc8fcee00ebab59620340132657c58cd0f25004133aa30d22
Flow Network Security	**LCM:** lcm_flow_pc_4.1.0.tar.gz	**SHA256:**565e17a2d1335c2c61e7093d1e14954b077ab4a323b40b1af537a551f20871d2
Flow Virtual Networking	**LCM:** 4.0.0.tar.gz	**SHA256:** 14ebfe2139807a070b0ef4f04b7c0ab6cb2d534609a1d267a609b0d9e6d11970
Files	**Upgrade:** nutanix-afs-el8.5-release-afs-5.0.0.1-stable-8da0965291d7453229238d58dc1abc3f09f4031d.qcow2	**SHA256:**86635e87ef0313606c1dcee5c9451a11a4a6182cf8619e878544774f9bc140f7
	LCM: lcm_file_server_5.0.0.1.tar.gz	**SHA256:**72a4bbc00a17098c229a7fa794028cf736e7a1588e9b12a705953a84e8ab438a
Objects	**LCM:** objects-5.0.tar.gz	**SHA256:**f6d8384aab4800a92c0b9fe9eda2ed87b2368d5e2b88aff17e32dc633d1bc62b
Self-Service	Epsilon-3.8.1.1.zip	**SHA256:** f05b8af12c56daeeb7d2913417e8d90d76d5859cdecaba5368397d37714c5c78
Nutanix Database	**Install:** NDB-Server-build-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.qcow2	**SHA256:**0b83d4c5b7b02e568b37d2a19470b039336c33f9c7f023005131003e7ce3ef5e

[2] LCM – Nutanix Lifecycle Manager

Component	Filename	Hash
	Upgrade: era_upgrade_bundle-2.5.5-e6a22438d6f5bdbda5f6c72e910e113d22655c6d.zip	**SHA256:**84fdca9a59319e9bfeff2540f8e045c2cbe916269cfe16bca6548d9c63be7ea1

1.5.1.2 Guidance Documentation

The following PDF formatted guides, listed in Table 3, are publicly available for download from the Nutanix website at https://www.nutanix.com/trust/compliance-and-certifications/common-criteria-auditorevaluation:

Table 3 – Guidance Documentation

Short Reference	Document Name	Description
[AAAG]	*Nutanix Acropolis Advanced Administration Guide AOS 6.8 May 20, 2024*	Contains information on how to maintain and configure the TOE.
[AHV_GUIDE]	*AHV Administration Guide AHV 6.8 May 21, 2024*	
[SEC_GUIDE]	*Security Guide AOS Security 6.8 May 17, 2024*	Contains information on securing the TOE.
[PC_ADMIN]	*Prism Central Admin Center Guide Prism pc.2024.2 April 29, 2025*	Contains information on how to use the web console.
[PC_INFRA]	*Prism Central Infrastructure Guide Prism pc.2024.2 April 17, 2025*	Contains information on how to use the web console.
[API_REF_v1]	*Acropolis v1 API[3] Reference AOS 6.8 May 20, 2024*	Contains information on the REST[4] API interface.
[FVN_GUIDE]	*Flow Virtual Networking Guide Flow Virtual Networking pc.2024.2 April 21, 2025*	Contains usage information for the Flow Virtual Networking TOE component
[FNS_GUIDE]	*Flow Network Security Next-Gen Release Version 4.1.x Guide May 17, 2024*	Contains usage information for the Flow Network Security TOE component
[SS_GUIDE]	*Self-Service Administration and Operations Guide Self-Service 3.8.1.1 May 26, 2025*	Contains usage information for the Self-Service TOE component
[FILES_GUIDE]	*Nutanix Files User Guide Files 5.0 May 20, 2024*	Contains usage information for the Nutanix Files TOE component
[OBJECTS_GUIDE]	*Objects User Guide Objects 5.0 May 20, 2024*	Contains usage information for the Nutanix Objects TOE component
[NDB_GUIDE]	*Nutanix Database Service Administration Guide Nutanix Database Service (formerly Era) 2.5 March 15, 2024*	Contains usage information for the Nutanix Database Service TOE component
[AGD_SUPP]	*Nutanix Guidance Documentation Supplement v0.13 December 1, 2025*	Contains information for administrators, specific to the evaluated version of the TOE
[REST_3]	*Nutanix v3 API Reference*	Contains information on the v3 REST API interface.
[REST_4]	*Nutanix REST API v4 Document*	Contains information on the v4 REST API interface.
[PRISM_WEB]	*Prism Element Web Console Guide, Prism 6.8, May 20, 2024*	Contains usage information for the Prism Element interface

The [AGD_SUPP] can be downloaded through the following link https://www.nutanix.com/content/dam/nutanix/documents/certifications/nutanix-ncp-v68-guidance-supplement-v013.pdf. Its associated SHA-256 checksum is "59f36bdc4c97903607d11456223610056bd44b080606aa4c1825df7c18c3864b"

[3] API – Application Programming Interface
[4] REST – Representational State Transfer

1.5.2 Logical Scope

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

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[5]
- Resource Utilization

1.5.2.1 Security Audit

The TOE records the actions of administrative users made through the management interfaces. Audit records can only be reviewed through Prism.

1.5.2.2 User Data Protection

The TOE enforces access controls on storage allocated to VMs. This storage is provided via NFSv4 shares. Access to this storage is controlled via an NFS whitelist that lists the IP address of every guest VM that is allowed to access the storage. The TOE also provides information controls so that only one client can modify virtual disk data at a time.

1.5.2.3 Identification and Authentication

The TOE requires users to identify and authenticate themselves to the TOE before granting permission to access any of the TOE's functionality.

1.5.2.4 Security Management

The TOE provides the following interfaces that administrative users can use to manage the TOE

- Prism Element GUI
- Prism Central GUI
- NDB GUI
- NDB CLI
- NDB REST API
- REST API v2
- REST API v3
- REST API v4

Administrative users can manage security attributes related to the Virtual Disk Access policy via these interfaces. The Virtual Disk Access policy allows any storage access requests (using the Storage Access Interface) to be made by default, unless a virtual disk is already locked. Administrative users can also manage accounts, containers,

[5] TSF – TOE Security Functionality

storage, virtual disks, and NTP servers. Administrative users can assume one of the administrative roles described in Section 7.1.4, or can be assigned multiple sets of privileges at once.

1.5.2.5 Protection of the TSF

The TOE maintains its full capabilities when a physical disk or host fails.

1.5.2.6 Resource Utilization

The TOE makes use of redundant hosts to prevent a single point of failure. The TOE remains fully operational with all data intact even if an entire physical disk or host fails.

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

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

- External cloud service integrations
- Custom user roles
- Nutanix cmdlets client
- Nutanix nCLI interface

2. Conformance Claims

This section and Table 4 provide the identification for any CC, PP, and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none);
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation Procedures (ALC_FLR.2)

3. Security Problem

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

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

3.1 Threats to Security

This section identifies the threats to the IT[6] assets against which protection is required by the TOE or by the security environment. The threat agents are divided into three categories:

- Attackers who are not administrative users: They have public knowledge of how the TOE operates and are assumed to possess a low skill level, limited resources to alter TOE configuration settings or parameters, and no physical access to the TOE.
- Administrative users: They have extensive knowledge of how the TOE operates and are assumed to possess a high skill level, moderate resources to alter TOE configuration settings or parameters, and physical access to the TOE. (Administrative users are, however, assumed not to be willfully hostile to the TOE.)
- Natural threats: There are threats to the TSF that are a natural byproduct of the systems that compose the TOE, such as electromagnetic interference on a line during transmission of user data.

All are assumed to have a low level of motivation. The IT assets requiring protection are the TSF and user data saved on or transitioning through the TOE and the hosts on the protected network. Removal, diminution, and mitigation of the threats are through the objectives identified in Section 4. Table 5 lists the applicable threats.

Table 5 – Threats

Name	Description
T.DATA_CORRUPTION	User data and configuration data could become corrupted due to hardware failure or incorrect system operations.
T.IMPROPER_SERVER	An administrative user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.
T.NO_AUDIT	An administrative user or attacker may perform security-relevant operations on the TOE without being held accountable for them.

3.2 Organizational Security Policies

There are no Organizational Security Policies (OSPs) defined for this ST.

[6] IT – Information Technology

3.3 Assumptions

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

Table 6 – Assumptions

Name	Description
A.CONNECTIVITY	It is assumed that the TOE environment will be configured in such a way as to allow administrative users to access the information stored on the TOE.
A.INTERNAL_STORAGE_NETWORK	The network that the TOE uses for storage transfer is intended to be an internal private network that is protected from access by entities outside of the organization. External access to storage services are blocked by the TOE environment.
A.INTERNAL_USERS	It is assumed that internal users accessing the storage on the TOE reside on the internal network and are not careless, negligent, or willfully hostile with regard to their access of the TOE.
A.LOCATE	It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrative users only.
A.NOEVIL	It is assumed that the administrative users who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.PROACTIVE	It is assumed that the administrators of the TOE’s operating environment conduct proactive checking of all systems and media traversed by the communication between administrative systems and the TOE.
A.TIME	It is assumed that the TOE environment will provide the time for the TOE from a reliable source.

4. Security Objectives

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

4.1 Security Objectives for the TOE

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

Table 7 – Security Objectives for the TOE

Name	Description
O.ADMIN	The TOE must provide a method for administrative users to manage the TOE.
O.AUDIT	The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrative users with the ability to review the audit trail in order to identify when misconfigurations have occurred.
O.AUTHENTICATE	The TOE must authenticate administrative users before granting them access to TOE functionality that can affect the enforcement of security functionality provided by the TOE.
O.FAULT_TOLERANCE	The TOE must be resilient against host or disk failures that might affect the security of the information it contains.
O.USER_DATA	The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 8 – IT Security Objectives

Name	Description
OE.CONNECT	Administrative users will configure the TOE environment so that administrative users have the proper network support to be able to access data on the TOE.
OE.INTERNAL_STORAGE_NETWORK	The TOE environment must limit access to the TOE from external entities such that only internal hosts can access the NFS storage functionality provided by the TOE.
OE.PROPER_NAME_ASSIGNMENT	Each guest VM running on top of AHV, that accesses storage on the TOE, must provide accurate unique server identifiers for itself.
OE.SECURE_COMMUNICATION	The TOE environment must provide un-tampered communications between systems connected to the TOE.

Name	Description
OE.TIME	The TOE environment must ensure that the time is provided to the TOE from a reliable source.

4.2.2 Non-IT Security Objectives

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

Table 9 – Non-IT Security Objectives

Name	Description
NOE.INTERNAL_USERS	Sites using the TOE shall ensure that internal users are not careless, negligent, or willfully hostile.
NOE.NOEVIL	Sites using the TOE shall ensure that administrative users are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
NOE.PHYSICAL	The TOE will be used in a physically secure site that protects it from interference and tampering by un-trusted subjects.

5. Extended Components

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

5.1 Extended TOE Security Functional Components

There are no extended SFRs defined for this ST.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

6. Security Requirements

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

6.1 Conventions

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

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

- Completed assignment statements are identified using [*italicized text within brackets*].
- Completed selection statements are identified using [underlined text within brackets].
- Completed assignment statements within a selection statement are identified using [*underlined and italicized text within brackets*].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FDP_ACC.1(a) Subset access control (Virtual Disk Access) would be the first iteration and FDP_ACC.1(b) Subset access control (Role Based Access Control) would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 10 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 10 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit Data Generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_ACC.1(a)	Subset access control (Virtual Disk Access)		✓		✓
FDP_ACC.1(b)	Subset access control (Role Based Access Control)		✓		✓
FDP_ACF.1(a)	Security attribute based access control (Virtual Disk Access)		✓		✓
FDP_ACF.1(b)	Security attribute based access control (Role Based Access Control)		✓		✓
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_UAU.2(a)	User authentication before any action (General)			✓	✓

Name	Description	S	A	R	I
FIA_UAU.2(b)	User authentication before any action (NDB)			✓	✓
FIA_UID.2(a)	User identification before any action (General)			✓	✓
FIA_UID.2(b)	User identification before any action (NDB)			✓	✓
FMT_MSA.1(a)	Management of security attributes (Virtual Disk Access)	✓	✓		✓
FMT_MSA.1(b)	Management of security attributes (Role Based Access Control)	✓	✓		✓
FMT_MSA.3(a)	Static attribute initialization (Virtual Disk Access)	✓	✓		✓
FMT_MSA.3(b)	Static attribute initialization (Role Based Access Control)	✓	✓		✓
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of Management Functions		✓		
FMT_SMR.1(a)	Security roles (General)		✓	✓	✓
FMT_SMR.1(b)	Security roles (NDB)		✓	✓	✓
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.2	Limited fault tolerance		✓		

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

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. [*all configuration changes made via management interfaces related to management of the Virtual Disk Access SFP, management of accounts, management of containers, management of virtual disks, and management of virtual machines*].

FAU_GEN.1.2

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

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*the following:*
  - *Operation Message*
  - *Entity*

- *Percent*
- *Status*
- *Create Time*
- *Duration*

].

FAU_SAR.1 Audit review

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1

The TSF shall provide [*administrative users with access to Prism*] with the capability to read [*all information*] 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.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control (Virtual Disk Access)

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(a).1

The TSF shall enforce the [*Virtual Disk Access SFP*] on [

Subjects:

- *Guest VMs*

Objects:

- *NFS share*

Operations:

- *Read, write*

].

FDP_ACC.1(b) Subset access control (Role Based Access Control)

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1(b).1

The TSF shall enforce the [*Role Based Access Control SFP*] on [

Subjects: TOE users

Objects: Prism entities

Operations: read, write].

FDP_ACF.1(a) Security attribute based access control (Virtual Disk Access)

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1(a).1

The TSF shall enforce the [*Virtual Disk Access SFP*] to objects based on the following: [

Subject (Guest VM) attributes:

- *VM Name*
- *Host ID*[7]

Object (NFS share) attributes:

- *(Container) Name*
- *Maximum Capacity*
- *NFS whitelist*

].

FDP_ACF.1(a).2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*If the guest VM's IP address is on the NFS whitelist, then access is allowed. Otherwise, access is denied*].

FDP_ACF.1(a).3

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

FDP_ACF.1(a).4

The TSF shall explicitly deny access of subjects to objects based on the [*If the maximum capacity is reached, access is denied*].

FDP_ACF.1(b) Security attribute based access control (Role Based Access Control)

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialisation

FDP_ACF.1(b).1

The TSF shall enforce the [*Role Based Access Control SFP*] to objects based on the following: [

- *Subject security attributes for TOE users: Role*
- *Object security attributes for: Entity permissions*

].

FDP_ACF.1(b).2

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*TOE users are granted access to entities based on roles*].

FDP_ACF.1(b).3

[7] ID – Identifier

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

FDP_ACF.1(b).4

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

FDP_IFC.1 Subset information flow control

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

The TSF shall enforce the [*Virtual Disk Locking SFP*] on [

Subjects:

- *Clients*[8]

Information:

- *Virtual Disks*

Operations:

- *Write*
- *Execute*

].

FDP_IFF.1 Simple security attributes

Dependencies: FDP_IFC.1 Subset information flow control

FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1

The TSF shall enforce the [*Virtual Disk Locking SFP*] based on the following types of subject and information security attributes: [

Subject (Processes) attributes:

- *Process ID*
- *Hostname*
- *Guest VM IP address*
- *Idle time*

Information attributes:

- *Virtual Disk ID*
- *Virtual disk lock*

].

[8] Clients are processes on guest VMs that access storage provided by the TOE.

FDP_IFF.1.2

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [*If the process (identified by process ID, hostname, and guest VM IP address) is designated in the virtual disk lock, access is allowed. Otherwise, access is denied*].

FDP_IFF.1.3

The TSF shall enforce the [*If the virtual disk does not currently have a virtual disk lock issued, the process may obtain a virtual disk lock from a leader host*[9]*. If the process idle time is 10 minutes, then the disk lock is released*].

FDP_IFF.1.4

The TSF shall explicitly authorize an information flow based on the following rules: [*no other rules*].

FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: [*no other rules*].

6.2.3 Class FIA: Identification and Authentication

FIA_UAU.2(a) User authentication before any action (General)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2(a).1

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

FIA_UAU.2(b) User authentication before any action (NDB)

Hierarchical to: FIA_UAU.1 Timing of authentication

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.2(b).1

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

FIA_UID.2(a) User identification before any action (General)

Hierarchical to: FIA_UID.1 Timing of identification

FIA_UID.2(a).1

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

FIA_UID.2(b) User identification before any action (NDB)

Hierarchical to: FIA_UID.1 Timing of identification

[9] A leader host is a host in the cluster that is responsible for issuing virtual disks locks.

FIA_UID.2(b).1

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

6.2.4 Class FMT: Security Management

FMT_MSA.1(a) Management of security attributes (Virtual Disk Access)

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(a).1

The TSF shall enforce the [*Virtual Disk Access SFP*] to restrict the ability to [change_default, query, modify] the security attributes [*VM name, host ID, (container) name, maximum capacity, NFS whitelist*] to [*Super Admin and Prism Admin roles*].

FMT_MSA.1(b) Management of security attributes (Role Based Access Control)

Dependencies: [FDP_ACC.1 Subset access control, or

FDP_IFC.1 Subset information flow control]

FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MSA.1(b).1

The TSF shall enforce the [*Role Based Access Control SFP*] to restrict the ability to [change_default, query, modify, create, delete] the security attributes [*entity permissions*] to [*the Super Admin and Prism Admin roles*].

FMT_MSA.3(a) Static attribute initialization (Virtual Disk Access)

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3(a).1

The TSF shall enforce the [*Virtual Disk Access SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(a).2

The TSF shall allow the [*Super Admin and Prism Admin roles*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.3(b) Static attribute initialization (Role Based Access Control)

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3(b).1

The TSF shall enforce the [*Role Based Access Control SFP*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3(b).2

The TSF shall allow the [*Super Admin and Prism Admin roles*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MTD.1 Management of TSF data

Dependencies: FMT_SMR.1 Security Roles

FMT_SMF.1 Specification of Management Functions

FMT_MTD.1.1

The TSF shall restrict the ability to [query, modify, delete] the [*accounts, containers, virtual machines, and virtual disks*] to [*the Super Admin and Prism Admin roles*].

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions: [

- *Configure Virtual Disk Access SFP attributes*
- *Manage accounts*
- *Manage containers*
- *Manage storage and virtual disks*
- *Manage the system time*
- *Management of virtual machines*
- *Manage Flow Network Security policies*
- *Manage Flow Virtual Networking policies*].

FMT_SMR.1(a) Security roles (General)

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1(a).1

The TSF shall maintain the roles [*Super Admin, Prism Admin, Prism Viewer, Self-Service Admin, Consumer, Developer, Operator, Project Admin, VPC Admin, Files Admin, Files Viewer, Flow Admin, Flow Viewer, Network Infra Admin, Cluster Viewer, Disaster Recovery Admin, Disaster Recovery Viewer, Objects Admin, Objects Viewer, File Server Security Admin, File Server Share Admin, Monitoring Admin, Monitoring Viewer, Action Service User, Category Viewer, Category Admin, CSI System, Kubernetes Data Services System, Kubernetes Infrastructure Provision, Storage Admin, Storage Viewer, Objects Editor, Flow Policy Author, Virtual Machine Viewer, Virtual Machine Operator, Virtual Machine Admin, Cluster Admin, User Admin, Backup Admin, and Viewer* [10]] **for management interfaces**.

FMT_SMR.1(a).2

[10] An administrative user can have one or more of these roles.

The TSF shall be able to associate users with roles.

FMT_SMR.1(b) Security roles (NDB)

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1(b).1

The TSF shall maintain the roles [*Super Administrator, Infrastructure administrator, Database infrastructure administrator, and Database administrator* [11]] **for NDB management interfaces only**.

FMT_SMR.1(b).2

The TSF shall be able to associate users with roles.

6.2.5 Class FPT: Protection of the TSF

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1

The TSF shall preserve a secure state when the following types of failures occur: [

- *Failure of a single host in a multi-host*[12] *cluster*
- *Failure of one disk or up to all disks on a single host in a multi-host cluster*

].

6.2.6 Class FRU: Resource Utilization

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: [

- *Failure of a single host in a multi-host cluster*
- *Failure of one disk or up to all disks on a single host in a multi-host cluster*

].

[11] An administrative user can have one or more of these roles.

[12] Multi-host refers to clusters with two or more nodes or servers installed.

6.3 Security Assurance Requirements

This section defines the assurance requirements for the TOE. Assurance requirements are taken from the CC Part 3 and are EAL2+ augmented with ALC_FLR.2. Table 11 summarizes these requirements.

Table 11 – Assurance Requirements

Assurance Requirements	
Class ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
Class ALC: Life Cycle Support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM Coverage
	ALC_DEL.1 Delivery Procedures
	ALC_FLR.2 Flaw Reporting Procedures
Class ADV: Development	ADV_ARC.1 Security Architecture Description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
Class AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
Class ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing – Sample
Class AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

7. TOE Summary Specification

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

7.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to a security functionality. Hence, each security functionality is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functionality and rationalize that the security functionality satisfies the necessary requirements. Table 12 lists the security functionality and their associated SFRs.

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

TOE Security Functionality	SFR	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1(a)	Subset access control
	FDP_ACC.1(b)	Subset access control
	FDP_ACF.1(a)	Security attribute based access control
	FDP_ACF.1(b)	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_UAU.2(a)	User authentication before any action (General)
	FIA_UAU.2(b)	User authentication before any action (NBD)
	FIA_UID.2(a)	User identification before any action (General)
	FIA_UID.2(b)	User authentication before any action (NBD)
Security Management	FMT_MSA.1(a)	Management of security attributes
	FMT_MSA.1(b)	Management of security attributes
	FMT_MSA.3(a)	Static attribute initialization
	FMT_MSA.3(b)	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1(a)	Security roles (General)
	FMT_SMR.1(b)	Security roles (NDB)

TOE Security Functionality	SFR	Description
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.2	Limited fault tolerance

7.1.1 Security Audit

The TOE records audits for TSF-related actions from administrative users through the management interfaces that can only be viewed by administrative users via Prism. The audit functionality is started upon startup of the TOE and does not halt until the TOE is shutdown. Although the TOE does not audit the startup and shutdown of the audit function, it does audit the startup and shutdown of the TOE, thereby indicating when the audit function is started and stopped as well.

The TOE audit records contain the following information:

Table 13 – Audit Record Contents

Field	Content
Operation Message	A description of the action, including the outcome (success or failure) and the event type.
Entity	The TOE component that the operation was performed on
Percent	The completion percentage of the operation
Status	The status of the operation
Create Time	The date and time that the event occurred.
Duration	How long the operation took to complete

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

7.1.2 User Data Protection

Storage for the cluster is provisioned as units called containers which are created from one or more tiers of disk storage (storage pools). The TOE can provide access to containers via NFS shares, which provide access to storage to guest VMs on the network.

The TOE implements a Virtual Disk Access SFP that controls what storage guest VMs can access on the TOE. This SFP controls access based on an NFS whitelist stored on the TOE. Additionally, each NFS share is allocated a certain amount of storage space that, once reached, results in administrative users not being able to access additional storage.

The TOE enforces a Virtual Disk Locking SFP, which allocates access to Virtual Disks via a mechanism called virtual disk locking. Virtual disk locking occurs when a process on a guest VM requests access to storage represented by a virtual disk from the leader host. If the virtual disk is currently being accessed by a different process, then the TOE denies access to the requesting process until the current process goes inactive for ten minutes. If the virtual disk is not currently locked, then the leader host issues a lock specifying the process ID, hostname, and guest VM IP address of the requesting process. The lock allows exclusive access to the virtual disk until the process goes idle (stop sending requests) for ten minutes. The lock is automatically extended if the process becomes active again.

The Role Based Access Control SFP is used to govern access to the Prism management interface. The SFP determines which TOE users have access to query, create, change, or delete TOE management policies based on the role that is assigned to them. The roles define which management functions, known as "entities", TOE users have access to. TOE users must be assigned the role of Super Admin or Prism Admin to perform these actions. TOE users can be assigned multiple roles.

TOE Security Functional Requirements Satisfied: FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), FDP_IFC.1, FDP_IFF.1.

7.1.3 Identification and Authentication

Administrative users must identify and authenticate themselves to the TOE or the Nutanix Database Service before being granted access to any of the management functionality provided via the management interfaces.

TOE Security Functional Requirements Satisfied: FIA_UAU.2(a), FIA_UAU.2(b), FIA_UID.2, FIA_UID.2(b).

7.1.4 Security Management

The Virtual Disk Access SFP has restrictive default values for security attributes used for enforcement of the SFP, and these default values can be overridden by administrative users. The VM name and ID of the host that the VM resides on must be entered by when creating a new VM. The container name must be entered when creating a new storage container. Maximum capacity is determined by the physical drives that are available in the storage pool, which is selected when creating the storage container. The NFS whitelist can be manually managed to permit access to NFS shares on the storage system or it can be automatically populated by the TOE. Administrative users with the Super Admin and Prism Admin roles have the ability to query, modify, delete or change default values of these security attributes.

Management of all TOE functionality takes place through the management interfaces:

- the TOE offers two web Graphical User Interfaces (GUIs), called Prism Element and Prism Central respectively
- The TOE also offers management of various services via REST API v2, v3, and v4
- the Nutanix Database Service (NDB) leverages a GUI, CLI, and REST API specific to NDB, referred to as the NDB GUI, NDB CLI, and NDB REST API respectively

Prism offers various pages for managing accounts, containers, storage, virtual disks, Flow Network Security policies, Flow Virtual Networking Policies, and the NTP server for the system time. Administrative users with the Super Admin and Prism Admin roles may query, modify, or delete data related to these areas depending on their assigned roles.

The following roles exist for the Prism Central interface and are governed by the Role Based Access Control SFP and are available only in Prism Central:

- The **Super Admin** role provides all of the Prism Admin functionality plus the ability to manage authentication methods, create local accounts, and change local account passwords. Administrative users can assume multiple roles simultaneously.
- The **Prism Admin** role provides the ability to modify all settings excluding anything related to authentication and creating accounts, and managing recovery plans.
- The **Prism Viewer** role provides read-only access to all settings and cannot open the console on VMs.

Additionally, the following table defines additional roles and their purposes:

Table 14 – Additional Roles and Purposes

Roles	Purpose
Self-Service Admin	Super user / administrator for Self-Service
Consumer	Project role that launches new blueprints and runs actions on apps

Roles	Purpose
Developer	Project role that creates / launches blueprints (RBAC rules), and runs actions on apps based on roles assigned in projects
Operator	Project role with minimum access and can only run actions against existing apps
Project Admin	Has full control of a project, which implements RBAC in Self-Service
VPC Admin	Manages VPC networking: create/update/delete networks
Files Admin	Administrator role for Files
Files Viewer	Auditor role for Files
Flow Admin	Administrator role for Flow
Flow Viewer	Auditor role for Flow
Network Infra Admin	Manages the network infrastructure on the AHV network stack
Cluster Viewer	Auditor role for Clusters
Disaster Recovery Admin	Administrator role for Disaster Recover (DR) with access to DR operations
Disaster Recovery Viewer	Auditor role for Disaster Recovery
Objects Admin	Can view information, perform administrative tasks, and create or modify Objects
Objects Viewer	Auditor role for Objects
File Server Security Admin	All File Server security related permissions
File Server Share Admin	All File Server security related permissions
Monitoring Admin	Full access to perform all Monitoring operations
Monitoring Viewer	View access to all API in Monitoring
Action Service User	Basic Playbook access for all users
Category Viewer	View access for category object
Category Admin	Full access for category object
CSI System	Full access for Kubernetes cluster infrastructure resources for CSI
Kubernetes Data Services System	Full access for Kubernetes cluster infrastructure resources for Kubernetes Data Services
Kubernetes Infrastructure Provision	Access for Kubernetes cluster infrastructure VMs resources
Storage Admin	Storage admin of a Nutanix deployment. This user can view and perform actions on Storage entities.
Storage Viewer	View access for Storage entities.
Objects Editor	Edit access to Object store operations.
Flow Policy Author	Full Access to flow operations, except categories provisioning

Roles	Purpose
Virtual Machine Viewer	View access for Virtual Machines.
Virtual Machine Operator	Gives access for day-to-day activities on Virtual Machines.
Virtual Machine Admin	Full access to Virtual Machines.

The Prism Element interface offers the following roles: User Admin, Cluster Admin, Backup Admin, and Viewer. All Prism Element accounts have the Viewer role by default and can be assigned to multiple roles. The permissions of each role are as follows:

- **Cluster Admin** allows the user to view information and perform any administrative task (but not create or modify user accounts).
- **User Admin** allows the user to view information, perform any administrative task, and create or modify user accounts. (Checking this box automatically selects the Cluster Admin box to indicate that this user has full permissions. However, a user administrator has full permissions regardless of whether the Cluster Admin box is checked.)
- **Backup Admin** allows the user to perform backup-related administrative tasks. This role does not have permission to perform cluster or user administrative tasks.

Leaving all the boxes unchecked assigns the **Viewer** role, which allows the user to view information, but it does not provide permission to perform cluster or user-administrative administrative tasks.

The NDB management interfaces include the following roles:

- **Super Administrator**
- **Infrastructure administrator**
- **Database administrator**
- **Database infrastructure administrator**

NDM users are associated with these roles when accessing NDB management interfaces.

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

7.1.5 Protection of the TSF

In the event of a host or disk failure, the TOE maintains a secure state by continuing to offer all of its functionality in the event of:

- Failure of a single host in a multi-host cluster
- Failure of one or up to all disks on a host in a multi-host cluster

This is possible because the TOE stores metadata for each virtual disk on three different hosts and data for each virtual disk on two different hosts for full-host redundancy. Additionally, the TOE uses Nutanix's Distributed Storage Fabric (DSF) that stripes data across mirrored arrays preventing data loss from the failure of a single disk.

TOE Security Functional Requirements Satisfied: FPT_FLS.1.

7.1.6 Resource Utilization

The TOE duplicates virtual disk data across multiple hosts to provide redundancy in the event of:

- Failure of a single host in a multi-host cluster
- Failure of one or up to all disks on a host in a multi-host cluster

This allows the TOE to remain fully operational in the event that one of these components fails.

TOE Security Functional Requirements Satisfied: FRU_FLT.2.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 5.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 15 provides a mapping of the objectives to the threats they counter.

Table 15 – Threats: Objectives Mapping

Threats	Objectives	Rationale
T.DATA_CORRUPTION User data and configuration data could become corrupted due to hardware failure or incorrect system operations.	O.ADMIN The TOE must provide a method for administrative users to manage the TOE.	O.ADMIN mitigates this threat by allowing administrative users to properly configure the mechanisms of the TOE that prevent data corruption.
	O.USER_DATA The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.	O.USER_DATA mitigates this threat by providing mechanisms to protect the configuration and user data that has been entrusted to the TOE against unauthorized modifications as a result of race conditions.
	O.FAULT_TOLERANCE The TOE must be resilient against host or disk failures that might affect the security of the information it contains.	O.FAULT_TOLERANCE mitigates this threat by ensuring that the TOE is capable of maintaining a secure state and offering its full set of functionalities in the event of a host or disk failure.
T.IMPROPER_SERVER An administrative user or attacker could attempt to bypass the access controls provided by the TOE by using one of the systems connected to the TOE.	O.ADMIN The TOE must provide a method for administrative users to manage the TOE.	O.ADMIN mitigates this threat by allowing administrative user to properly configure the mechanisms of the TOE designed to control the access and information flow control policies.
	OE.PROPER_NAME_ASSIGNMENT Each guest VM within the TOE environment, that runs on top of AHV, must provide accurate unique server identifiers for itself.	OE.PROPER_NAME_ASSIGNMENT mitigates this threat by ensuring that the unique server identifiers provided by AHV (for its hosted VMs) to other components of the TOE are accurate.
	O.USER_DATA The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.	O.USER_DATA mitigates this threat by providing adequate mechanisms to give only authorized servers access to configuration data.

Threats	Objectives	Rationale
	OE.SECURE_COMMUNICATIONS The TOE environment must provide un-tampered communications between systems connected to the TOE.	OE.SECURE_COMMUNICATIONS mitigates this threat by ensuring that all communications with the TOE are un-tampered for administration of the TOE, internal TOE communications, and data sent to or from the TOE. This is accomplished by proactive checking of all systems and media traversed by the communication between administrative systems and the TOE.
	O.AUTHENTICATE The TOE must authenticate administrative users before granting them access to TOE functionality that can affect the enforcement of security functionality provided by the TOE.	O.AUTHENTICATE mitigates this threat by ensuring that administrative users are authenticated before allowing access to TOE management functionality.
T.NO_AUDIT An administrative user or attacker may perform security-relevant operations on the TOE without being held accountable for them.	O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrative users with the ability to review the audit trail in order to identify when misconfigurations have occurred.	O.AUDIT mitigates this threat by ensuring that an audit trail of management events on the TOE is preserved. Accurate timestamps are also provided for all audit records, allowing order of events to be preserved.

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 16 gives a mapping of assumptions and the environmental objectives that uphold them.

Table 16 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.NOEVIL It is assumed that the administrative users who manage the TOE are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	NOE.NOEVIL Sites using the TOE shall ensure that administrative users are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.	NOE.NOEVIL upholds this assumption by ensuring that administrative users are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.
A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrative users only.	NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by un-trusted subjects.	NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided for the TOE.
A.CONNECTIVITY It is assumed that the TOE environment will be configured in such a way as to allow administrative users to access the information stored on the TOE.	OE.CONNECT Administrative users will configure the TOE environment so that administrative users have the proper network support to be able to access data on the TOE.	OE.CONNECT upholds this assumption by ensuring that the TOE environment is configured appropriately to allow users to access information stored on the TOE.

Assumptions	Objectives	Rationale
A.TIME It is assumed that the TOE environment will provide the time for the TOE from a reliable source.	OE.TIME The TOE environment must ensure that the time is provided to the TOE from a reliable source.	OE.TIME upholds this assumption by ensuring that the time will be provided to the TOE from a reliable source.
A.INTERNAL_STORAGE_NETWORK The network that the TOE uses for storage transfer is intended to be an internal private network that is protected from access by entities outside of the organization. External access to storage services are blocked by the TOE environment.	OE.INTERNAL_STORAGE_NETWORK The TOE environment must limit access to the TOE from external entities such that only internal hosts can access the NFS storage functionality provided by the TOE.	OE.INTERNAL_STORAGE_NETWORK upholds this assumption by ensuring that only internal hosts can access the NFS storage provided by the TOE.
A.INTERNAL_USERS It is assumed that internal users accessing the storage on the TOE reside on the internal network and are not careless, negligent, or willfully hostile with regard to their access of the TOE.	NOE.INTERNAL_USERS Sites using the TOE shall ensure that internal users are not careless, negligent, or willfully hostile.	NOE.INTERNAL_USERS upholds this assumption by ensuring that the internal users accessing TOE storage are not careless, negligent, or willfully hostile.
A.PROACTIVE It is assumed that the administrators of the TOE's operating environment conduct proactive checking of all systems and media traversed by the communication between administrative systems and the TOE.	O.USER_DATA The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.	O.USER_DATA upholds this assumption by ensuring that systems are properly and proactively configured in a secure manner.

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended SFRs defined for this ST.

8.4 Rationale for Extended TOE Security Assurance Requirements

There are no extended SARs defined for this ST.

8.5 Security Requirements Rationale

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

8.5.1 Rationale for Security Functional Requirements of the TOE Objectives

Table 17 shows a mapping of the objectives and the SFRs that support them.

Table 17 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative users to manage the TOE.	FMT_MSA.1(a) Management of security attributes	This requirement meets O.ADMIN by specifying the security attributes of the TOE that can be modified and which administrative roles can modify them.
	FMT_MSA.1(b) Management of security attributes	This requirement meets O.ADMIN by specifying the security attributes of the TOE that can be modified and which administrative roles can modify them.
	FMT_MSA.3(a) Static attribute initialization	This requirement meets O.ADMIN by specifying that restrictive values are used by the access controls enforced by the TOE and specifying the administrative roles that can set alternate values.
	FMT_MSA.3(b) Static attribute initialization	This requirement meets O.ADMIN by specifying that restrictive values are used by the access controls enforced by the TOE and specifying the administrative roles that can set alternate values.
	FMT_MTD.1 Management of TSF data	This requirement meets O.ADMIN by specifying what roles can operate on TSF data contained in the TOE configuration.
	FMT_SMF.1 Specification of Management Functions	This requirement meets O.ADMIN by specifying each of the management functions that are used to securely manage the TOE. These functions are provided by the TOE management interfaces.
	FMT_SMR.1(a) Security roles (General)	This requirement meets O.ADMIN by specifying the administrative roles defined to govern management of the TOE on the general interfaces.
	FMT_SMR.1(b) Security roles (NDB)	This requirement meets O.ADMIN by specifying the administrative roles defined to govern management of the TOE on the NDM management interfaces.
O.AUDIT The TOE must record events of security relevance at the "not specified" level of audit. The TOE must provide authorized administrative users with the ability to review the audit trail in order to identify when misconfigurations have occurred.	FAU_GEN.1 Audit Data Generation	This requirement meets O.AUDIT by requiring the TOE to produce audit records for the system security events.
	FAU_SAR.1 Audit review	This requirement meets O.AUDIT by requiring the TOE to make the recorded audit records available for review
O.AUTHENTICATE The TOE must authenticate administrative users before granting them access to TOE functionality that can affect the enforcement of security functionality provided by the TOE.	FIA_UAU.2(a) User authentication before any action (General)	This requirement meets O.AUTHENTICATE by requiring TOE administrative users to authenticate their claimed identities before the TOE will perform any action on their behalf via the management interfaces.
	FIA_UAU.2(b) User authentication before any action (NBD)	This requirement meets O.AUTHENTICATE by requiring NBD administrative users to authenticate their claimed identities before the NBD will perform any action on their behalf via the management interfaces.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UID.2(a) User identification before any action (General)	This requirement meets O.AUTHENTICATE by requiring administrative users to identify themselves before the TOE perform any actions on their behalf.
	FIA_UID.2(b) User identification before any action (NBD)	This requirement meets O.AUTHENTICATE by requiring administrative users to identify themselves before NBD perform any actions on their behalf.
O.FAULT_TOLERANCE The TOE must be resilient against host or disk failures that might affect the security of the information it contains.	FPT_FLS.1 Failure with preservation of secure state	This requirement meets O.FAULT_TOLERANCE by ensuring that the TOE maintains a secure state in the event of a disk or host failure.
	FRU_FLT.2 Limited fault tolerance	This requirement meets O.FAULT_TOLERANCE by ensuring that the TOE does not lose any functionality in the event of a disk or host failure.
O.USER_DATA The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.	FDP_ACC.1(a) Subset access control	This requirement meets O.USER_DATA by enforcing an access control policy that ensures that only authorized devices gain access to user and configuration data within the TOE.
	FDP_ACC.1(b) Subset access control	This requirement meets O.USER_DATA by enforcing an access control policy that ensures that only authorized devices gain access to user and configuration data within the TOE.
	FDP_ACF.1(a) Security attribute based access control	This requirement meets O.USER_DATA by providing access control functionality to manage access to user and configuration data within the TOE.
	FDP_ACF.1(b) Security attribute based access control	This requirement meets O.USER_DATA by providing access control functionality to manage access to user and configuration data within the TOE.
	FDP_IFC.1 Subset information flow control	This requirement meets O.USER_DATA by enforcing an information flow control policy that ensures that access to user data is granted in a controlled manner to prevent data anomalies.
	FDP_IFF.1 Simple security attributes	This requirement meets O.USER_DATA by providing information flow control functionality to manage data flows to user data within the TOE.

8.5.2 Security Assurance Requirements Rationale

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

The augmentation of ALC_FLR.2 was chosen to give greater assurance of the developer's on-going flaw remediation processes.

8.5.3 Dependency Rationale

The SFRs in this ST satisfy all of the required dependencies listed in the Common Criteria, applicable PPs, and SFRs explicitly stated in this ST. Table 18 lists each requirement to which the TOE claims conformance and indicates whether the dependent requirements are included. As the table indicates, all dependencies have been met.

Table 18 – Functional Requirements Dependencies

SFR	Dependency	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	Although FPT_STM.1 is not claimed, the TOE acquires the time from a trusted NTP server in the TOE environment.
FAU_SAR.1	FAU_GEN.1	✓	
FDP_ACC.1(a/b)	FDP_ACF.1(a/b)	✓	
FDP_ACF.1(a/b)	FDP_ACC.1(a/b)	✓	
	FMT_MSA.3(a/b)	✓	
FDP_IFC.1	FDP_IFF.1	✓	
FDP_IFF.1	FDP_IFC.1	✓	
	FMT_MSA.3	✓	There is no management available for the information flow control policy beyond the automatic assignment, release, and renewal of virtual disk locks. Therefore, FMT_MSA.3 does not need to be met for this requirement.
FIA_UAU.2(a/b)	FIA_UID.1(a/b)	✓	Although FIA_UID.1 is not claimed, FIA_UID.2(a/b), which is hierarchical to FIA_UID.1, is.
FIA_UID.2(a/b)	None	Not applicable	
FMT_MSA.1(a/b)	FMT_SMF.1	✓	

	FMT_SMR.1	✓	FMT_SMR.1(a) maps to FMT_MSA.1(a)
			FMT_SMR.1(b) maps to FMT_MSA.1(b)

	FDP_ACC.1(a/b)	✓	

FMT_MSA.3(a/b)	FMT_MSA.1(a/b)	✓	FMT_MSA.1(a) maps to FMT_MSA.3(a)
			FMT_MSA.1(b) maps to FMT_MSA.3(b)

	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1(a/b)	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1(a/b)	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2(a/b), which is hierarchical to FIA_UID.1, is.
FPT_FLS.1	None	Not applicable	
FRU_FLT.2	FPT_FLS.1	✓	

9. Acronyms

Table 19 defines the acronyms used throughout this document.

Table 19 – Acronyms

Acronym	Definition
AHV	Acropolis Hypervisor
AOS	Acropolis Operating System
CC	Common Criteria
CLI	Command Line Interface
CM	Configuration Management
CVM	Controller Virtual Machine
DSF	Distributed Storage Fabric
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HA	High Availability
HTTPS	Hypertext Transfer Protocol Secure
IT	Information Technology
JRE	Java Runtime Environment
NCI	Nutanix Cloud Infrastructure
nCLI	Nutanix Command Line Interface
NCP	Nutanix Cloud Platform
NDB	Nutanix Database Service
NFS	Network Filesystem
NTP	Network Time Protocol
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Functionality Policy
SFR	Security Functional Requirement

Acronym	Definition
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSP	TOE Security Policy
VM	Virtual Machine

10. Appendix A – Supported Hardware Platforms

The following Nutanix hardware platforms are supported by the TOE software:

- NX-1065-G8
- NX-1065-G9
- NX-1065N-G8
- NX-1175S-G8
- NX-1175S-G9
- NX-3035-G9
- NX-3060-G8
- NX-3060-G9
- NX-3155G-G8
- NX-3155GN-G8
- NX-3155-G9
- NX-3170-G8
- NX-3170N-G8
- NX-8035-G8
- NX-8035N-G8
- NX-8150-G8
- NX-8150-G9
- NX-8150N-G8
- NX-8155-G8
- NX-8155N-G8
- NX-8155-G9
- NX-8155A-G9
- NX-8170-G8
- NX-8170N-G8
- NX-8170-G9

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Circle
Suite 210
Fairfax, VA 22033
United States of America

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