

Nutanix, Inc.

Nutanix Enterprise Cloud (AOS & AHV)

v5.15

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 0.7

Prepared for:

NUTANIXTM

Nutanix, Inc.
1740 Technology Drive
Suite 400
San Jose, CA 95110
United States of America

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

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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

Table of Contents

1.	Introduction	4
1.1	Purpose	4
1.2	Security Target and TOE References	4
1.3	Product Overview	5
1.3.1	Smart Metadata	6
1.3.2	Data Availability	6
1.3.3	Data Efficiency	7
1.3.4	VM Support	7
1.3.5	Management Interfaces	7
1.4	TOE Overview	8
1.5	TOE Environment	9
1.6	TOE Description	9
1.6.1	Physical Scope	9
1.6.2	Logical Scope	11
1.6.3	Product Physical/Logical Features and Functionality not included in the TOE	13
2.	Conformance Claims	14
3.	Security Problem	15
3.1	Threats to Security	15
3.2	Organizational Security Policies	15
3.3	Assumptions	16
4.	Security Objectives	17
4.1	Security Objectives for the TOE	17
4.2	Security Objectives for the Operational Environment	17
4.2.1	IT Security Objectives	17
4.2.2	Non-IT Security Objectives	18
5.	Extended Components	19
5.1	Extended TOE Security Functional Components	19
5.2	Extended TOE Security Assurance Components	19
6.	Security Requirements	20
6.1	Conventions	20
6.2	Security Functional Requirements	20
6.2.1	Class FAU: Security Audit	21
6.2.2	Class FDP: User Data Protection	21
6.2.3	Class FIA: Identification and Authentication	23
6.2.4	Class FMT: Security Management	24
6.2.5	Class FPT: Protection of the TSF	25
6.2.6	Class FRU: Resource Utilization	26
6.2.7	Class FTA: TOE Access	26
6.3	Security Assurance Requirements	26
7.	TOE Summary Specification	28
7.1	TOE Security Functionality	28
7.1.1	Security Audit	28
7.1.2	User Data Protection	29

- 7.1.3 Identification and Authentication 29
- 7.1.4 Security Management 30
- 7.1.5 Protection of the TSF 30
- 7.1.6 Resource Utilization 31
- 7.1.7 TOE Access..... 31
- 8. Rationale..... 32
 - 8.1 Conformance Claims Rationale 32
 - 8.2 Security Objectives Rationale 32
 - 8.2.1 Security Objectives Rationale Relating to Threats 32
 - 8.2.2 Security Objectives Rationale Relating to Policies 33
 - 8.2.3 Security Objectives Rationale Relating to Assumptions..... 33
 - 8.3 Rationale for Extended Security Functional Requirements 34
 - 8.4 Rationale for Extended TOE Security Assurance Requirements..... 34
 - 8.5 Security Requirements Rationale..... 34
 - 8.5.1 Rationale for Security Functional Requirements of the TOE Objectives..... 35
 - 8.5.2 Security Assurance Requirements Rationale 36
 - 8.5.3 Dependency Rationale 37
- 9. Acronyms 38

List of Figures

- Figure 1 – Physical TOE Boundary 10

List of Tables

- Table 1 – ST and TOE References4
- Table 2 – Guidance Documentation 11
- Table 3 – CC and PP Conformance 14
- Table 4 – Threats 15
- Table 5 – Assumptions..... 16
- Table 6 – Security Objectives for the TOE 17
- Table 7 – IT Security Objectives..... 17
- Table 8 – Non-IT Security Objectives..... 18
- Table 9 – TOE Security Functional Requirements 20
- Table 10 – Assurance Requirements 26
- Table 11 – Mapping of TOE Security Functionality to Security Functional Requirements..... 28
- Table 12 – Audit Record Contents..... 29
- Table 13 – Threats: Objectives Mapping..... 32
- Table 14 – Assumptions: Objectives Mapping 33
- Table 15 – Objectives: SFRs Mapping..... 35
- Table 16 – Functional Requirements Dependencies 37
- Table 17 – Acronyms 38

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The TOE is the Nutanix, Inc. (Nutanix) Nutanix Enterprise Cloud (AOS & AHV) v5.15 and will hereafter be referred to as the TOE throughout this document. The TOE is comprised of the Acropolis Operating System (AOS), which is running on a Controller Virtual Machine (CVM), and the Acropolis Hypervisor (AHV) that contains the CVM. 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.
- 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	<i>Nutanix, Inc. Nutanix Enterprise Cloud (AOS & AHV) v5.15 Security Target</i>
ST Version	Version 0.7
ST Author	Corsec Security, Inc.
ST Publication Date	July 16, 2020

Nutanix Enterprise Cloud (AOS & AHV) v5.15

TOE Reference

Nutanix Enterprise Cloud (AOS & AHV) v5.15 consists of the following software components:

- Acropolis Operating System (AOS) v5.15 LTS
- Acropolis Hypervisor (AHV) v20170830.395

1.3 Product Overview

The Product Overview provides the introduction to the overall product offering.

Nutanix Enterprise Cloud is a virtualization platform composed of networked hosts that can host guest VMs offering services to users. These guest VMs can be used for any application the users of the server require, such as web, email, or others. Nutanix Enterprise Cloud also offers storage for those VMs to use when offering services. The unification of storage and virtualization on a single platform eliminates the need for a separate storage network. This cuts overhead and administrative costs for operating a virtualization platform. Additionally, Nutanix Enterprise Cloud scales linearly to meet increased guest VM processing or storage needs by allowing additional hosts to be added to the cluster individually. This compounds the overhead-reducing effects inherent in a virtualization platform, which reduces hardware needs dramatically as compared to a traditional server infrastructure.

Nodes are hardware boards housed within one or more chassis running the AOS and AHV software and provide all of the functionality for the cluster. A node is a blade server with a complete instantiation of server hardware (processor, memory, storage, and network) that supports the virtualization and storage needs of the system's users. Alternatively, generic servers can be used in place of nodes to run the AOS and AHV software. Each host provides storage and virtualization services to users, with multiple hosts being used for redundancy.

Nutanix Enterprise Cloud makes use of the existing physical network infrastructure to connect each host together using standard network protocols, rather than a private physical network. Nutanix Enterprise Cloud provides its own private subnet for internal cluster communications. This subnet is typically configured to be inaccessible by entities other than the clustered hosts.

The foundational unit for Nutanix Enterprise Cloud is a grouping of three hosts within a cluster, each of which contains processors, memory, and local storage (a PCIe¹ Solid State Drive (SSD), SSDs, and Hard Disk Drives (HDDs)) and runs AHV. Each one hosts a Nutanix Enterprise Cloud CVM that enables the pooling of local storage from all hosts in the cluster.

When a guest VM running on a host submits a write request through AHV, that request is sent to the CVM of that host. To provide a rapid response to the guest VM, this data is first stored on the PCIe SSD device, within a subset of storage called the Heat-Optimized Tiering (HOT) Cache. This cache is rapidly distributed across the 10 GbE² network to other PCIe SSD devices in the cluster. HOT Cache data is periodically transferred to persistent storage within the cluster. Data is written locally for performance and replicated on multiple hosts for high availability.

When the guest VM sends a read request through AHV, the CVM first checks local storage for a copy of the data. If the host does not contain a local copy, then the CVM will read across the network from another host in the

¹ PCIe – Peripheral Component Interconnect Express

² GbE – Gigabit Ethernet

Nutanix Enterprise Cloud (AOS & AHV) v5.15

cluster that does contain a copy. As remote data is accessed, it is migrated to storage devices on the current host, so that future read requests are local.

The Nutanix Distributed Storage Fabric (DSF) is at the core of Nutanix Enterprise Cloud. DSF manages all metadata and data and enables core features. DSF is the underpinning architectural element that connects the storage, compute resources, CVM, and AHV. It also provides full Information Lifecycle Management (ILM), including localizing data to the optimal host. The software portion of the solution is referred to as AOS.

1.3.1 Smart Metadata

Metadata is distributed among all hosts in the cluster in order to eliminate any single point of failure and to allow scalability that increases linearly with cluster growth. The metadata is partitioned using a consistent hashing scheme to minimize the redistribution of keys during cluster-sizing modifications.

The system enforces strong consistency through a distributed consensus algorithm. Quorum-based leadership election eliminates potential “split brain” scenarios, which ensures strict consistency of configuration data.

1.3.2 Data Availability

DSF was designed from the ground up to be extremely fault resilient. It ensures data availability in the event of a host, controller, or disk failure. DSF creates redundant copies of the data and keeps the replicas (copies) on separate hosts. Writes to system data are logged in the fastest disk tier that includes PCIe SSDs. These can be configured to replicate to another controller before the write is committed. If a host or disk failure occurs, DSF automatically rebuilds data copies to ensure a copy of the data remains available as much as possible.

Nutanix Enterprise Cloud is designed to recover automatically from loss of physical components. By leveraging the distributed nature of the cluster, Nutanix Enterprise Cloud proactively scrubs data to resolve disk or data errors. If a CVM fails, all disk I/O³ requests are automatically forwarded to another CVM until the local CVM becomes available again. This technology is completely transparent to AHV, and the guest VMs continue to run normally. In the case of a host failure, an HA event is automatically triggered and the VMs fail-over to another host within the cluster. Nutanix Enterprise Cloud localizes disk I/O operations by migrating data to the virtual machine’s local CVM. Simultaneously, data is re-replicated to maintain a consistent number of replicas.

DSF provides build-in converged-backup and disaster recovery capabilities. The converged-backup capabilities leverage array-size snapshots⁴ and clones⁵, which are performed using sub-host-level change-tracking at the VM and file level. The snapshots and clones are instantaneous, and thin provisioning maintains very low overhead. These capabilities also support AHV array offload⁶ capabilities.

Snapshots can be configured on a standard schedule and can be replicated to remote sites using array-side replication⁷. This replication is configurable at the VM level, and only the sub-host-level changes are shipped to the remote replication site.

³ I/O – Input/Output

⁴ Snapshots refer to point-in-time backups of files that exist as they were at the time the snapshot was taken.

⁵ Clones are copies of VMs.

⁶ Array offload refers to distributing computational workloads to the storage array rather than having the client perform these tasks.

⁷ Array-side replication refers to the storage system’s ability to copy snapshots.

1.3.3 Data Efficiency

A core design principle of Nutanix Enterprise Cloud is data localization. It keeps data proximate to the VM and allows write I/O operation to be localized on that same host. If a VM migrates to another host in an event such as Distributed Resource Scheduling (DRS), the data automatically follows the VM, so it maintains the highest performance. After a certain number of read requests made by a VM to a CVM that resides on another host, ILM transparently moves the remote data to the local CVM so the read I/O is served locally, instead of traversing the network.

Nutanix Enterprise Cloud incorporates HOT, which leverages multiple tiers of storage and optimally places data on the tier that provides the best performance. The architecture was built to support local disks attached to the CVM (PCIe SSD, SSD, and HDD) as well as remote (NAS⁸) and cloud-based source targets. The tiering logic is fully extensible, allowing new tiers to be dynamically added and extended. Nutanix Enterprise Cloud continuously monitors data-access patterns to determine whether access is random, sequential, or a mixed workload. Random I/O workloads are maintained in a PCIe SSD tier to minimize seek times. Sequential workloads are automatically placed into the HDD tier to improve endurance.

The most frequently accessed data (hot data) resides on the highest performance tier (PCIe SSD). That tier is not just a cache – it is a truly persistent tier for both read and write operations. The next hottest data is placed on the SSD tier, which serves as spillover for the highest performance tier (PCIe SSD), as well as Quality of Service (QoS)-controlled data. Cold data sits on HDDs, which is the highest-capacity and most economical tier.

DSF array-side compression capabilities work in combination with ILM. For sequential workloads, data is compressed during the write operation using in-line compression. For batch workloads, post-process compression adds significant value as data is compressed once it becomes idle and ILM has moved it down to the HDD tier. All compression configurations are carried out at a container level and operate at a granular VM and file level. Decompression is done at the sub-host level to ensure precise granularity. The operations are monitored by the ILM process, which proactively moves frequently accessed data up to a higher performance data tier.

1.3.4 VM Support

Nutanix Enterprise Cloud 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, KVM⁹, or Hyper-V. Administrative users can backup guest VM data along with user data through replication functionality available through Nutanix Enterprise Cloud.

1.3.5 Management Interfaces

The product offers a Command Line Interface (CLI) called the Nutanix CLI (nCLI), a web Graphical User Interface (GUI) called Prism that can be used to maintain and configure Nutanix Enterprise Cloud, and a Representational state transfer (REST) Application Programming Interface (API) that can be used to programmatically run system

⁸ NAS – Network Attached Storage

⁹ KVM – Kernel-based Virtual Machine

Nutanix Enterprise Cloud (AOS & AHV) v5.15

administration commands. The CLI is run over Secure Hypertext Transfer Protocol (HTTPS) and is downloaded from Prism, which also communicates via HTTPS. Once retrieved, nCLI is run as a standalone application on the administrative user's workstation.

1.4 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 the security functionality defined below. The TOE consists of all the Nutanix software that makes-up Nutanix Enterprise Cloud in a three host cluster. Note that all of the hardware is considered to be within the TOE environment. Nutanix Enterprise Cloud v5.15 consists of the following software components:

- Acropolis Operating System (AOS) v5.15 LTS
- Acropolis Hypervisor (AHV) v20170830.395

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 NFS¹⁰ 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 provides reliable time stamps that are used to preserve the order of events for the audit records.

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 three administrative roles defined for the TOE: User Administrator, Cluster Administrator, and View-Only. 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. During authentication via Prism, only obscured feedback is provided to the administrative user. The TOE also maintains passwords for local accounts and their associated usernames. Passwords must be at least 8 characters long.

¹⁰ NFS – Network File System

Nutanix Enterprise Cloud (AOS & AHV) v5.15

1.5 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 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 offer services to end users. The guests VMs 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.

The TOE requires administrative users to access storage and services through appropriate clients from their workstations that are general-purpose computers. An example of this is Postman, a REST API client used for collaboration in API development. Administrative users should access Prism through a modern graphical browser. Administrative users should access nCLI on the TOE using the local nCLI client¹¹ that can be downloaded via Prism and installed on the workstation. Java Runtime Environment (JRE) version 5.0 or higher is required for nCLI.

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 NTP¹² server that can provide reliable time stamps to the TOE.

1.6 TOE Description

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

1.6.1 Physical Scope

The physical scope of the TOE includes the Nutanix AOS v5.15 LTS and AHV v20170830.395 software components. 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 NX-1365-G7 hardware platform running Nutanix Enterprise Cloud 5.15. Note that the NX-1365-G7 is the same as the NX-1065-G7 but the “3” in place of the “0” means that there are 3 nodes in the chassis. Nutanix Enterprise Cloud was not tested on, but is capable of running on, other host hardware and is derived from a single image with different functionality enabled or disabled to support the host’s hardware. The following host hardware can be used with the TOE software:

- NX-1065-G7
- NX-1175S-G7

¹¹ It should be noted that the local nCLI client provides similar functionality to a web browser in the sense that it is only used to display data returned from the TOE and pass commands to nCLI running on the TOE. Therefore, the local nCLI client is considered to be a required component of the TOE environment and not part of the TOE.

¹² NTP – Network Time Protocol

Nutanix Enterprise Cloud (AOS & AHV) v5.15

- NX-3060-G7
- NX-3155-G7
- NX-3170-G7
- NX-8170-G7
- NX-8150-G7
- NX-8155-G7
- NX-8035-G7
- DX360-4-G10
- DX360-8-G10
- DX360-10-G10-NVMe
- DX380-8-G10
- DX380-12-G10
- DX380-24-G10
- DX560-24-G10
- DX2200-DX170R-G10-12LFF
- DX2200-DX190R-G10-12LFF
- DX2600-DX170R-G10-24SFF
- DX4200-G10-24LFF
- DX8000-DX910

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

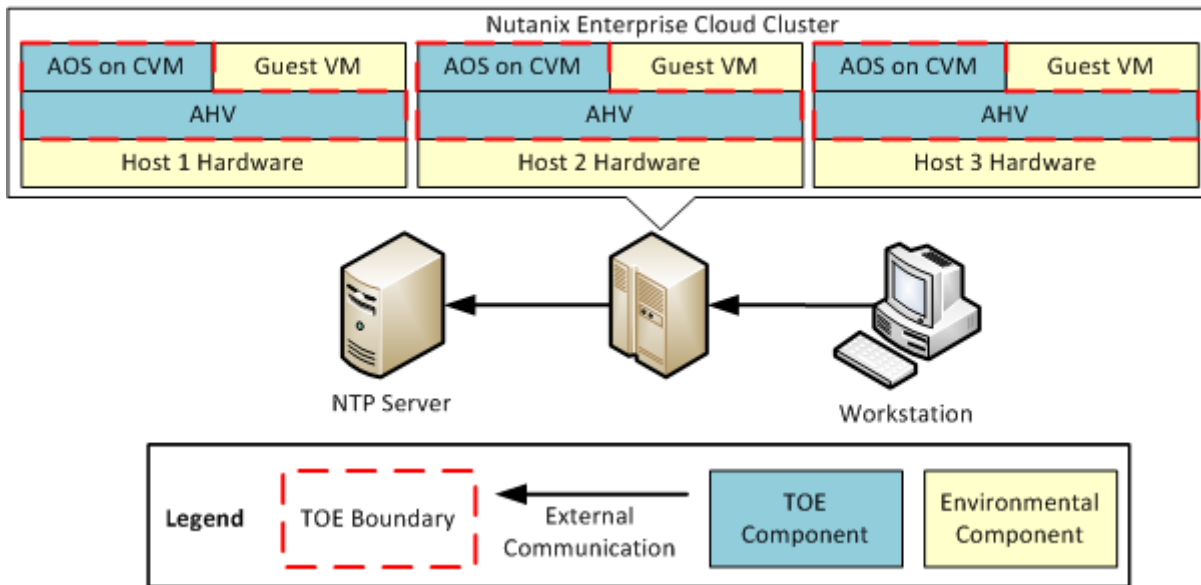


Figure 1 – Physical TOE Boundary

The TOE boundary includes the Nutanix-developed AOS and AHV of the three-host deployment for Nutanix Enterprise Cloud. Any third-party source code or software that Nutanix has modified for Nutanix Enterprise Cloud is also considered to be TOE software. The TOE boundary does not include the following environmental components shown above in Figure 1:

Nutanix Enterprise Cloud (AOS & AHV) v5.15

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

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

- Local nCLI client running on the workstation
- REST API client running on the workstation
- Web browser running on the workstation
- Management tools or products used to access AHV

It should be noted that 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.

1.6.1.1 Guidance Documentation

Table 2 lists the PDF¹³ formatted guides that are required reading and part of the TOE.

Table 2 – Guidance Documentation

Document Name	Description
<i>Nutanix AOS 5.15 Acropolis Advanced Administration Guide March 31, 2020</i>	Contains information on how to maintain and configure the TOE.
<i>Nutanix AHV 5.15 AHV Administration Guide March 31, 2020</i>	
<i>Nutanix AOS 5.15 Command Reference March 31, 2020</i>	Lists the commands available from nCLI along with a description of how to use each command.
<i>Nutanix AOS 5.15 Acropolis Advanced Setup Guide March 31, 2020</i>	Contains information for the initial setup of the TOE.
<i>Nutanix Security 5.15 Security Guide March 31, 2020</i>	Contains information on securing the TOE.
<i>Nutanix Prism 5.15 Prism Web Console Guide March 31, 2020</i>	Contains information on how to use the web console.
<i>Nutanix AOS 5.15 Acropolis v1 API Reference March 31, 2020</i>	Contains information on the REST API interface. An online reference is also available at https://www.nutanix.dev/api-reference/ .
<i>Nutanix, Inc. Nutanix Enterprise Cloud (AOS & AHV) v5.15 Guidance Supplement v0.4</i>	Contains information regarding specific configuration for the TOE evaluated configuration.

1.6.2 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

¹³ PDF – Portable Document Format

Nutanix Enterprise Cloud (AOS & AHV) v5.15

- Identification and Authentication
- Security Management
- Protection of the TSF¹⁴
- Resource Utilization
- TOE Access

1.6.2.1 Security Audit

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

1.6.2.2 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 IP¹⁵ 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.

1.6.2.3 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. Administrative users are required to define strong passwords for themselves. The TOE stores each local account's username and password. While logging into Prism, the TOE obscures passwords for administrative users.

1.6.2.4 Security Management

The TOE provides the REST API, Prism, and nCLI that administrative users can use to manage the TOE. 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 to be made by default, unless a virtual disk is already locked. Administrative users can also manage accounts, containers, storage, virtual disks, and NTP servers. Administrative users can assume the User Administrator role, Cluster Administrator role, View-Only role or can be assigned multiple sets of privileges at once.

1.6.2.5 Protection of the TSF

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

1.6.2.6 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.

1.6.2.7 TOE Access

The TOE provides the capability for administrative users to log out from Prism and nCLI.

¹⁴ TSF – TOE Security Functionality

¹⁵ IP – Internet Protocol

Nutanix Enterprise Cloud (AOS & AHV) v5.15

1.6.3 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:

- Guest VMs are not included within the TOE boundary and none of the functionality they provide has been tested as part of this evaluation.
- The management interfaces for the hypervisor are not included within the TOE boundary and should be considered part of the IT environment.
- SSH connections to the TOE are excluded from the evaluated configuration.
- The cryptography used in the HTTPS connections for the management via management interfaces has not been tested as part of this evaluation.
- The data efficiency claims in section 1.3.3 have not been explicitly evaluated as part of this evaluation.
- Host hardware will not be part of the TOE boundary and none of the features it provides will be included in the evaluated configuration.
- PowerShell cmdlets are not included within the TOE boundary and none of the functionality they provide has been tested as part of this evaluation.

2. Conformance Claims

This section and Table 3 provide the identification for any CC, PP, and EAL package conformance claims. A rationale is provided for any extensions or augmentations to the conformance claims. The rationales for any CC and PP conformance claims can be found in Section 8.1.

Table 3 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	<i>Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 5, April 2017; CC Part 2 conformant; CC Part 3 conformant; PP claim (none); Parts 2 and 3 Interpretations of the Common Evaluation Methodology (CEM) as of 2020-2-10 were reviewed, and no interpretations apply to the claims made in this ST.</i>
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 IT¹⁶ 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 4 below lists the applicable threats.

Table 4 – 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.

¹⁶ IT – Information Technology
Nutanix Enterprise Cloud (AOS & AHV) v5.15

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 5 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 5 – 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 administrative 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.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 6 below.

Table 6 – 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. Administrative users must use secure credentials to access TOE functionality.
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 7 below lists the IT security objectives that are to be satisfied by the environment.

Table 7 – 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 within the TOE environment that accesses storage on the TOE must provide accurate unique server identifiers for itself.

Name	Description
OE.SECURE_COMMUNICATION	The TOE environment must provide un-tampered communications between systems connected to the TOE.
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 8 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 8 – 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].
- Refinements are identified using **bold text**. Any text removed is stricken (Example: ~~TSF Data~~) and should be considered as a refinement.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 9 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement.

Table 9 – TOE Security Functional Requirements

Name	Description	S	A	R	I
FAU_GEN.1	Audit data generation	✓	✓		
FAU_SAR.1	Audit review		✓		
FDP_ACC.1	Subset access control		✓		
FDP_ACF.1	Security attribute based access control		✓		
FDP_IFC.1	Subset information flow control		✓		
FDP_IFF.1	Simple security attributes		✓		
FIA_ATD.1	User attribute definition		✓		
FIA_SOS.1	Verification of secrets		✓		
FIA_UAU.2	User authentication before any action				
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UID.2	User identification before any action				
FMT_MSA.1	Management of security attributes	✓	✓		
FMT_MSA.3	Static attribute initialisation	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		

Name	Description	S	A	R	I
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓	✓	
FPT_FLS.1	Failure with preservation of secure state		✓		
FRU_FLT.2	Limited fault tolerance		✓		
FTA_SSL.4	User-initiated termination				

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

6.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1

The TSF shall be able to generate an audit record of the following auditable events:

- a. Start-up and shutdown of the audit functions;
- b. All auditable events, for the [not specified] level of audit; and
- c. [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:

- a. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- b. For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [no other information].

FAU_SAR.1 Audit review

Hierarchical to: No other components.

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 Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1

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

- *Guest VMs*
- Objects:*
- *NFS share*
-].

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1

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

Subject (Guest VM) attributes:

- *VM Name*
- *Host ID¹⁷*

Object (NFS share) attributes:

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

].

FDP_ACF.1.2

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

FDP_ACF.1.3

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

FDP_ACF.1.4

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

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

Dependencies: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1

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

Subjects:

- *Clients¹⁸*

Information:

- *Virtual Disks*

Operations:

- *Write*
- *Execute*

].

¹⁷ ID – Identifier

¹⁸ Clients are processes on guest VMs that access storage provided by the TOE.

FDP_IFF.1 Simple security attributes**Hierarchical to: No other components.****Dependencies: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialization****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*

].

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 host¹⁹. 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_ATD.1 User attribute definition**Hierarchical to: No other components.****Dependencies: No dependencies****FIA_ATD.1.1**

The TSF shall maintain the following list of security attributes belonging to individual users: [username, password].

FIA_SOS.1 Verification of secrets**Hierarchical to: No other components.****Dependencies: No dependencies****FIA_SOS.1.1**

The TSF shall provide a mechanism to verify that secrets meet [the requirement of being at least 8 characters long].

¹⁹ A leader host is a host in the cluster that is responsible for issuing virtual disks locks.

FIA_UAU.2 User authentication before any action**Hierarchical to:** FIA_UAU.1 Timing of authentication**Dependencies:** FIA_UID.1 Timing of identification**FIA_UAU.2.1**

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

FIA_UAU.7 Protected authentication feedback**Hierarchical to:** No other components.**Dependencies:** FIA_UAU.1 Timing of authentication**FIA_UAU.7.1**

The TSF shall provide only [*obfuscated feedback in the form of bullets via Prism*] to the user while the authentication is in progress.

Application note: FIA_UAU.7 only applies to Prism. The REST API and nCLI rely on clients installed on the workstation to obscure their passwords.

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.

6.2.4 Class FMT: Security Management

FMT_MSA.1 Management of security attributes**Hierarchical to:** No other components.**Dependencies:** [FDP_ACC.1 Subset access control or
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles**FMT_MSA.1.1**

The TSF shall enforce the [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 [*the User Administrator and Cluster Administrator roles*].

FMT_MSA.3 Static attribute initialization**Dependencies:** FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security roles

FMT_MSA.3.1

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.3.2

The TSF shall allow the [*User Administrator and Cluster Administrator 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

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

FMT_MTD.1.1

The TSF shall restrict the ability to [*query, modify, delete*] the [*accounts, containers, virtual machines, and virtual disks*] to [*the User Administrator and Cluster Administrator roles*].

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: [

- *Configure Virtual Disk Access SFP attributes*
- *Manage accounts*
- *Manage containers*
- *Manage storage and virtual disks*
- *Manage the system time*
- *Management of virtual machines*

].

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 [*User Administrator, Cluster Administrator, View-Only*²⁰] **for management interfaces.**

FMT_SMR.1.2

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

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: [

- *Failure of a single host in a multi-host*²¹ *cluster*
- *Failure of one disk or up to all disks on a single host in a multi-host cluster*

].

²⁰ An administrative user can have one or more of these roles.

²¹ Multi-host refers to clusters with two or more nodes or servers installed.

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

].

6.2.7 Class FTA: TOE Access

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_SSL.4.1

The TSF shall allow user-initiated termination of the user’s own interactive session.

6.3 Security Assurance Requirements

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 10 summarizes these requirements.

Table 10 – 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 ²² 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

²² CM – Configuration Management
Nutanix Enterprise Cloud (AOS & AHV) v5.15

Assurance Requirements	
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 11 lists the security functionality and their associated SFRs.

Table 11 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Functionality	SFR ID	Description
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_SAR.1	Audit review
User Data Protection	FDP_ACC.1	Subset access control
	FDP_ACF.1	Security attribute based access control
	FDP_IFC.1	Subset information flow control
	FDP_IFF.1	Simple security attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_SOS.1	Verification of secrets
	FIA_UAU.2	User authentication before any action
	FIA_UAU.7	Protected authentication feedback
	FIA_UID.2	User identification before any action
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security roles
Protection of the TSF	FPT_FLS.1	Failure with preservation of secure state
Resource Utilization	FRU_FLT.2	Limited fault tolerance
TOE Access	FTA_SSL.4	User-initiated termination

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 Nutanix Enterprise Cloud (AOS & AHV) v5.15

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 12 – 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.

TOE Security Functional Requirements Satisfied: FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FDP_IFF.1.

7.1.3 Identification and Authentication

The TOE stores attributes of username and password for local accounts. Passwords stored within the TOE are in non-plaintext form. The TOE requires administrative users to define secure passwords when setting a password for their account. Secure passwords for the TOE must be at least 8 characters long.

Administrative users must identify and authenticate themselves to the TOE before being granted access to any of the management functionality provided via the management interfaces. Passwords are obfuscated with bullets when being typed into a login prompt on Prism.

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

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 User Administrator and Cluster Administrator 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. Prism offers various pages for managing accounts, containers, storage, virtual disks, and the NTP server for the system time. Likewise, nCLI and the REST API offer commands for managing these features. Administrative users with the User Administrator and Cluster Administrator roles may query, modify, or delete data related to these areas depending on their assigned roles.

The following roles are available for the management interfaces: User Administrator, Cluster Administrator, and View-Only. The View-Only role provides the ability to view all settings and cannot open the console on VMs. The Cluster Administrator role provides the ability to modify all settings excluding anything related to authentication and creating accounts. The User Administrator role provides all of the Cluster Administrator functionality plus the ability to manage authentication methods, create local accounts, and change local account passwords. Administrative users can assume multiple roles simultaneously.

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

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.

7.1.7 TOE Access

The TOE provides the ability for administrative users to terminate their sessions via Prism and nCLI. This can be accomplished through Prism by clicking the “logout” button and through nCLI by typing the `exit` command.

TOE Security Functional Requirements Satisfied: FTA_SSL.4.

8. Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 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 13 below provides a mapping of the objectives to the threats they counter.

Table 13 – 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 accesses storage on the TOE must provide accurate unique server identifiers for itself.	OE.PROPER_NAME_ASSIGNMENT mitigates this threat by ensuring that the unique server identifiers provided to the TOE are accurate.

Threats	Objectives	Rationale
	<p>O.USER_DATA The TOE must prevent unauthorized modifications to configuration and user data that it has been entrusted to protect.</p>	<p>O.USER_DATA mitigates this threat by providing adequate mechanisms to give only authorized servers access to configuration data.</p>
	<p>OE.SECURE_COMMUNICATIONS The TOE environment must provide untampered communications between systems connected to the TOE.</p>	<p>OE.SECURE_COMMUNICATIONS mitigates this threat by ensuring that all communications with the TOE are untampered for administration of the TOE, internal TOE communications, and data sent to or from the TOE.</p>
	<p>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. Administrative users must use secure credentials to access TOE functionality.</p>	<p>O.AUTHENTICATE mitigates this threat by ensuring that administrative users are authenticated before allowing access to TOE management functionality. This objective also ensures that strong passwords are used for administrative users' credentials.</p>
<p>T.NO_AUDIT An administrative user or attacker may perform security-relevant operations on the TOE without being held accountable for them.</p>	<p>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.</p>	<p>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.</p>

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

8.2.2 Security Objectives Rationale Relating to Policies

There are no OSPs defined for this ST.

8.2.3 Security Objectives Rationale Relating to Assumptions

Table 14 below gives a mapping of assumptions and the environmental objectives that uphold them.

Table 14 – Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
<p>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.</p>	<p>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.</p>	<p>NOE.NOEVIL upholds this assumption by ensuring that administrative users are not careless, negligent, or willfully hostile, are appropriately trained, and follow all guidance.</p>

Assumptions	Objectives	Rationale
<p>A.LOCATE It is assumed that the TOE is located within a controlled access facility and is physically available to authorized administrative users only.</p>	<p>NOE.PHYSICAL The TOE will be used in a physically secure site that protects it from interference and tampering by un-trusted subjects.</p>	<p>NOE.PHYSICAL upholds this assumption by ensuring that physical security is provided for the TOE.</p>
<p>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.</p>	<p>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.</p>	<p>OE.CONNECT upholds this assumption by ensuring that the TOE environment is configured appropriately to allow users to access information stored on the TOE.</p>
<p>A.TIME It is assumed that the TOE environment will provide the time for the TOE from a reliable source.</p>	<p>OE.TIME The TOE environment must ensure that the time is provided to the TOE from a reliable source.</p>	<p>OE.TIME upholds this assumption by ensuring that the time will be provided to the TOE from a reliable source.</p>
<p>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.</p>	<p>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.</p>	<p>OE.INTERNAL_STORAGE_NETWORK upholds this assumption by ensuring that only internal hosts can access the NFS storage provided by the TOE.</p>
<p>A.INTERNAL_USERS It is assumed that administrative 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.</p>	<p>NOE.INTERNAL_USERS Sites using the TOE shall ensure that internal users are not careless, negligent, or willfully hostile.</p>	<p>NOE.INTERNAL_USERS upholds this assumption by ensuring that the internal users accessing TOE storage are not careless, negligent, or willfully hostile.</p>

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

8.3 Rationale for Extended Security Functional Requirements

There are no extended 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 15 below shows a mapping of the objectives and the SFRs that support them.

Table 15 – Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ADMIN The TOE must provide a method for administrative users to manage the TOE.	FIA_ATD.1 User attribute definition	This requirement meets O.ADMIN by ensuring that administrative user attributes are maintained by the TOE.
	FMT_MSA.1 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 Static attribute initialisation	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 Security roles	This requirement meets O.ADMIN by specifying the administrative roles defined to govern management of the TOE.
	FTA_SSL.4 User-initiated termination	This requirement meets O.ADMIN by providing administrative users with the option to log out of an active session with the 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. Administrative users must use secure credentials to access TOE functionality.	FIA_SOS.1 Verification of secrets	This requirement meets O.AUTHENTICATE by requiring administrative users to defined secure passwords.
	FIA_UAU.2 User authentication before any action	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.

Objective	Requirements Addressing the Objective	Rationale
	FIA_UAU.7 Protected authentication feedback	This requirement meets O.AUTHENTICATE by preventing passwords from being read while typing them into the login prompts for the TOE management interfaces.
	FIA_UID.2 User identification before any action	This requirement meets O.AUTHENTICATE by requiring administrative users to identify themselves before the TOE 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 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 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 16 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 16 – Functional Requirements Dependencies

SFR ID	Dependencies	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	FDP_ACF.1	✓	
FDP_ACF.1	FDP_ACC.1	✓	
	FMT_MSA.3	✓	
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_ATD.1	None	Not applicable	
FIA_SOS.1	None	Not applicable	
FIA_UAU.2	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2, which is hierarchical to FIA_UID.1, is.
FIA_UAU.7	FIA_UAU.1	✓	Although FIA_UAU.1 is not claimed, FIA_UAU.2, which is hierarchical to FIA_UAU.1, is.
FIA_UID.2	None	Not applicable	
FMT_MSA.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
	FDP_ACC.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	None	Not applicable	
FMT_SMR.1	FIA_UID.1	✓	Although FIA_UID.1 is not claimed, FIA_UID.2, which is hierarchical to FIA_UID.1, is.
FPT_FLS.1	None	Not applicable	
FRU_FLT.2	FPT_FLS.1	✓	
FTA_SSL.4	None	Not applicable	

9. Acronyms

Table 17 defines the acronyms used throughout this document.

Table 17 – Acronyms

Acronym	Definition
AHV	Acropolis Hypervisor
AOS	Acropolis Operating System
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CLI	Command Line Interface
CM	Configuration Management
CVM	Controller Virtual Machine
DRS	Distributed Resource Scheduling
DSF	Distributed Storage Fabric
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
HA	High Availability
HDD	Hard Disk Drive
HOT	Heat-Optimized Tiering
HTTPS	Secure Hypertext Transfer Protocol
I/O	Input/Output
ID	Identifier
ILM	Information Lifecycle Management
IP	Internet Protocol
IT	Information Technology
JRE	Java Runtime Environment
KVM	Kernel-based Virtual Machine
NAS	Network Attached Storage
nCLI	Nutanix Command Line Interface
NFS	Network File System
NTP	Network Time Protocol
OSP	Organizational Security Policy
PCIe	Peripheral Component Interconnect Express

Acronym	Definition
PDF	Portable Document Format
PP	Protection Profile
QoS	Quality of Service
REST	Representational State Transfer
SAR	Security Assurance Requirement
SFP	Security Functional Policy
SFR	Security Functional Requirement
SSD	Solid State Drive
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VM	Virtual Machine

Prepared by:
Corsec Security, Inc.



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

Phone: +1 703 267 6050

Email: info@corsec.com

<http://www.corsec.com>
