Tintri, Inc.

Tintri VMstore v3.1.2.1

Security Target

Evaluation Assurance Level (EAL): EAL2+
Document Version: 1.4

Prepared for:

Tintri, Inc.
303 Ravendale Drive
Mountain View, CA 94043
United States of America

Phone: +1 650 810 8200
Email: info@tintri.com
http://go.tintri.com

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

Table of Contents

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Table of Figures

List of Tables

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the ST organization. The Target of Evaluation (TOE) is the Tintri VMstore v3.1.2.1, and will hereafter also be referred to as the TOE throughout this document. The TOE is the operating system and hardware platform of the Tintri VMstore storage appliance. Its features ensure that user data (vDisks[1], clones, and VM[2] backups) is protected and available to administrative users[3].

1.1 Purpose

This ST is divided into nine sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE, as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile, and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Requirements (Section 6) – Presents the SFRs and SARs met by the TOE.
- TOE Security Specification (Section 7) – Describes the security functions provided by the TOE that satisfy the security functional requirements 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 and terminology 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	Tintri, Inc. Tintri VMstore v3.1.2.1 Security Target
ST Version	Version 1.4
ST Author	Corsec Security, Inc.
ST Publication Date	8/10/2015
TOE Reference	Tintri VMstore v3.1.2.1

[1] vDisks – Virtual Disks
[2] VM – Virtual Machine
[3] The term "administrative users" refers to users and administrators that perform the management and monitoring tasks of the TOE.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3 Product Overview

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

The Tintri VMstore T800 series is a hybrid storage solution designed exclusively for VMs. It utilizes both flash-based solid-state drives (SSD) and hard-disk drives (HDD) for storage. The VMstore provides administrative users with a single view of all the VMs registered, allowing them to manage, monitor and control the VMs and their mounted vDisks without having detailed knowledge of the underlying storage infrastructure.

The VMstore T800 series (also referred to as VMstore or the VMstore appliance) consists of a 4U[4] storage and controller chassis with 24 hot-pluggable storage devices. The storage devices on the VMstore T820 are comprised of 14 SSDs and 10 HDDs, and the storage devices on the VMstore T850 and T880 are comprised of 11 SSDs and 13 HDDs. The VMstore appliance contains two storage controllers (hardware active-standby) that determine which storage devices contain the requested data, potentially compute the entire request from multiple devices, and return the data to the administrative user. The storage controllers can also determine the data access patterns for blocks of data, and move frequently-used data to the highest performing tier of storage. If there is duplicate data being stored, the controllers create pointers to common data. These storage controllers contain ports for administration, data, and optional replication networks, which are setup during initial configuration.

The VMstore storage appliance implements the Tintri FlashFirst™ Design to ensure that active data and metadata are kept in high performance flash. This design incorporates algorithms for inline deduplication, compression, and working set analysis. The Tintri File System monitors and controls I/O[5] for each vDisk to provide performance isolation. Based on the observed I/O characteristics of a vDisk, the VMstore working set analyzer stores cold parts of a VM and snapshots in HDDs and all active data is stored in SSDs. The VMstore also utilizes RAID[6] 6 software with real-time error correction for data protection on SSD and HDD, and features per-VM exportation, cloning, and snapshots to ensure the reliable backup and recovery of VMs.

The VMstore appliance's on-box management tools provide a Management GUI[7] via HTTPS[8], as well as management console access via KVM[9], SFTP[10] for software upgrades, SNMPv3[11] for network management, and SMTP[12] for email alerts. VMstore also has out-of-the box integration with VMware vCenter or Red Hat Enterprise Virtualization Manager. A single VMstore appliance can connect to up to 16 vCenter Servers or Virtualization Managers. In addition, Tintri provides customers with the option of implementing Tintri Global Center for the management of multiple VMstore appliances. Global Center enables administrative users to centrally monitor and control up to 32 VMstore systems and tens of thousands of VMs as one solution. The Global Center GUI provides end-to-end insight into individual VMs, key metrics on performance and capacity usage, and summary reports with up to one month's statistics for all controlled VMstore systems. The Global Center is a separate product and is not a part of the evaluated configuration.

[4] U – Unit
[5] I/O – Input/Output
[6] RAID – Redundant Array of Independent Disks
[7] GUI – Graphical User Interface
[8] HTTPS – Hypertext Transfer Protocol Secure
[9] KVM – Keyboard, Video, Mouse
[10] SFTP – Secure File Transfer Protocol
[11] SNMPv3 – Simple Network Management Protocol Version 3
[12] SMTP – Simple Mail Transfer Protocol

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.3.1 VM & vDisk Level Management

The Management GUI is used for initial configuration and provides administrative users with resource performance management and monitoring services including:

- Displaying graphs and statistics about VMs and vDisks
- Configuring and performing snapshot, cloning, and exportation services
- Pinning VMs or vDisks to flash
- Upgrading the Tintri Operating System software

Administrative users can view VMstore graphs and statistics regarding IOPS[13], throughput, latency, and flash hit ratio of VMs and vDisks. Graphs can be used to view trends in performance and to compare VMs or vDisks.

The VMstore snapshot schedule enables the VMstore to schedule snapshots (point in time read-only copies) of all VMs at regular, pre-determined times to provide data protection. Administrative users can also create clones, which are writable copies of existing VMs or snapshots. Data can be quickly restored by cloning a snapshot to a new VM. If snapshots are exported to a secondary VMstore, the exported snapshots can also be used for restoration purposes. Exportation allows a VM from one VMstore to be copied to another VMstore destination (displayed as a synthetic VM).

1.4 TOE Overview

The TOE Overview provides a context for the TOE evaluation by defining the specific evaluated configuration and TOE environment.

The TOE includes the Tintri Operating System of the Tintri VMstore storage appliance and the hardware platform that it runs on (models T820, T850, and and T880). The storage appliance has dual hardware controllers and each controller runs a separate copy of the Tintri Operating System.

The TOE enforces the VM HA Access Control Policy and the VM Migration Access Control Policy. The VM HA Access Control Policy is used during the exportation of VMs to other VMstore storage appliances. This policy ensures that copies of VMs are moved to other VMstore storage appliances if both of the storage appliances have the correct initiating IP[14] address, destination IP address, and shared authentication key. The VMs are copied to the target storage appliance with its associate security attributes including file owner, group owner, and permissions. The VM Migration Access Control Policy allows clients[15] to migrate VMs into the storage of the appliance if they have an allowed IP address that is on a stored NFS[16] white list.

Administrative users manage and monitor the VMs that are stored in the VMstore appliance by using the TOE's management GUI. Before authentication, administrative users can access API[17] version information and summary performance, alerts, and hardware status information using REST[18] API calls. Also, the use of the storage services and the exportation of VMs does not require authentication. Administrative users accessing the Management GUI can be authenticated locally or remotely using LDAP[19]. The TOE stores the local administrative user ID[20], roles, and passwords of administrative users. During authentication, the Management GUI provides obscured feedback. Administrative users can terminate their own sessions.

[13] IOPS – Input/Output Operations Per Second
[14] IP – Internet Protocol
[15] The term "clients" refers to the users migrating VMs and vDisks into the TOE using a hypervisor manager
[16] NFS – Network File System
[17] API – Application Programming Interface
[18] REST – Representational State Transfer
[19] LDAP – Lightweight Directory Access Protocol
[20] ID – Identifier

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Once an administrative user is identified and authenticated, the GUI is used to modify, delete, create, and provide restrictive default values for the NFS white list. Other management functions performed via the Management GUI include configuring administrative user accounts (which can only be modified, deleted, or created by authorized administrative users), snapshot services, and exportation services.

The security roles of the administrative users include the Super Admin, Storage Admin, and Read-Only User. Super Admins can perform all management tasks while Storage Admins can perform all management tasks except for managing administrative user accounts, and Read-Only Users can only monitor the system.

The TOE software includes a file system which processes read, write, and metadata requests and stores files to the HDD and SSD disks. The TOE utilizes RAID 6 software and keeps controllers in sync so that if a controller fails or two disks on a controller fail, the TOE preserves a secure state and all capabilities of the TOE are still operational.

The TOE runs a suite of self tests during initial start-up to demonstrate the correct operation of the TOE, and it provides reliable time stamps which are used for audit logs and to keep the active and standby controllers in sync.

Audit messages are generated by the TOE for administrative user actions (except read-only actions), system errors, and debug actions. These audit messages are stored as logs and can be reviewed by the administrative users but cannot be deleted or modified. The TOE overwrites the oldest stored audit records if the audit trail is full.

A diagram of the Tintri Operating System architecture appears in Figure 1. An acronym that appears in the figure but has not been previously defined is:

- QoS – Quality of Service

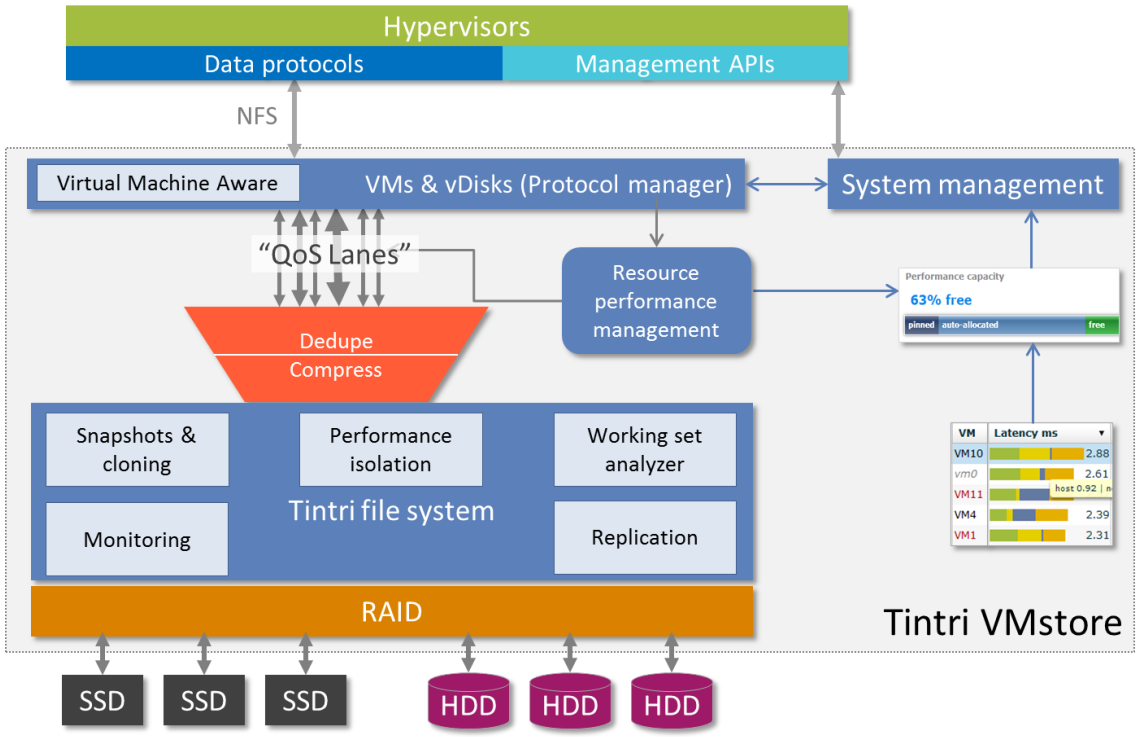

Figure 1 Tintri Operating System Diagram

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.4.1 Evaluated Configuration

The TOE boundary is depicted in the diagram below with a red dotted line. The TOE boundary encompasses the entire Tintri Operating System software image (a copy of the operating system runs on both controllers) and includes the T820, T850, and T880 hardware platforms on which the TOE executes. All functionality (except functionality listed in Section 1.5.3 below) of the product is included within the TOE boundary.

Figure 2 shows the details of the deployment configuration of the TOE:

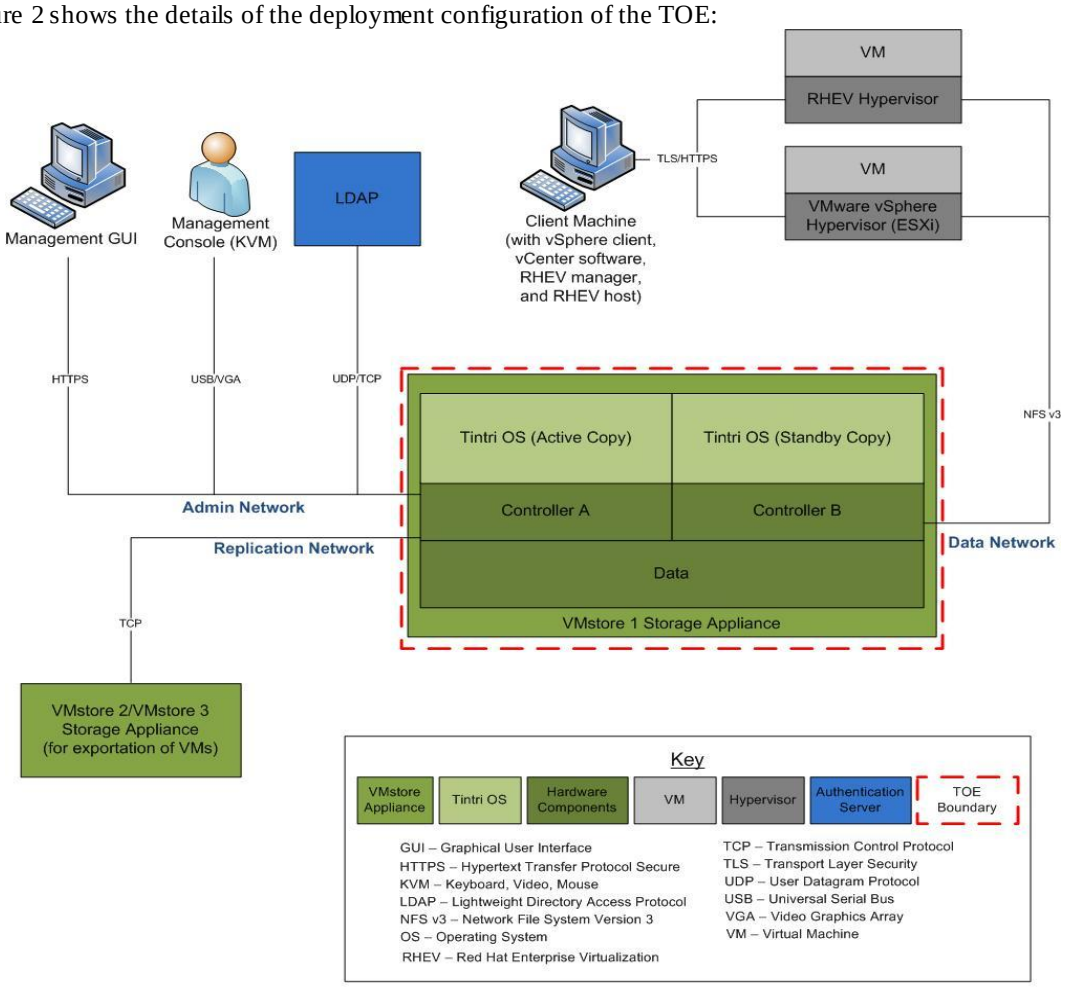

Figure 2 Deployment Configuration of the TOE

1.4.1.1 Management Interfaces

VMstore's management interface in the evaluated configuration is the web-based Management GUI.

1.4.2 TOE Environment

The TOE requires the following components to be properly configured and available in the operational environment:

- Three dual-controller Tintri VMstore appliances (two for exportation of VMs)

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

  - Rack Space: 4U[21] in a 19" four post square hole rack per appliance
  - Power Receptacles: These systems ship with NEMA[22] 5-15P[23] power cords, 110–240V[24] AC[25] auto-ranging power supplies, and adapter cables for shrouded IEC[26]320 C14 style plugs
  - Admin Network: six 1GbE[27] network cables (minimum three)
  - Data Network: six 10GbE network cables
  - Replication Network (for exportation of VMs): six 1GbE network cables
- Management Workstation with a browser, used to administer the TOE via GUI
- USB[28] Keyboard and Monitor or KVM Switch (required for initial configuration only) for Management Console
- LDAP Server
- VMware vSphere and Red Hat Enterprise Virtualization (RHEV) Hypervisors (on the client machine)

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 and Logical Scope

Figure 2 above illustrates the physical and logical scope and the physical boundary of the overall solution and ties together all of the components of the TOE and the TOE Environment. The TOE boundary includes the entire Tintri Operating System software image and the hardware platforms that it runs on.

The logical boundary of the TOE will be broken down into the following security classes which are further described in sections 6 and 7 of this ST. The logical scope also provides the description of the security features of the TOE.

The security functional requirements implemented by the TOE are usefully grouped under the following Security Function Classes:

- Security Audit
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF[29]
- Resource Utilization
- TOE Access

1.5.1.1 Security Audit

The TOE audits all administrative user actions (except read-only actions) and debug actions on the TOE's Management GUI. The debug logs store performance statistics, state dumps (recorded state of memory), internal and external events such as exportation of VMs, snapshot, and cloning information, garbage collection (memory manager), and other information useful for debugging problems. The TOE also audits

[21] U – Unit
[22] NEMA – National Electrical Manufacturers Association
[23] P - Plug
[24] V – Volts
[25] AC – Alternating Current
[26] IEC – International Electrotechnical Commission
[27] GbE – Gigabit Ethernet
[28] USB – Universal Serial Bus
[29] TSF – TOE Security Functionality

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

system errors regarding the physical malfunctions of the hardware platform. The TOE audit records contain at least the following information: date and time of the event, type of event, subject identity (if applicable), administrative user identity, and a message indicating the outcome (success or failure) of the event if applicable.

The TOE can provide audit review functions to all administrative users of the TOE, and protects the stored audit records in the audit trail by preventing unauthorized deletion or modification. Audit records are rotated based on time and capacity and the oldest stored audit records are overwritten if the audit trail is full.

1.5.1.2 User Data Protection

User Data Protection defines how administrative users connecting to the TOE are allowed to perform operations on VMs and their mounted vDisks.

Client access to objects controlled by the TOE is governed by the enforcement of the VM Migration Access Control Policy. This policy restricts access to the TOE via NFS v3 based on the host IP address. The VM HA Access Control policy is also enforced by the TOE when exporting VMs (with the VM's associated security attributes) outside of the TOE. Copies of VMs are created using snapshot information (from manually created, cloned, or scheduled snapshots) and cached data. Snapshots are logical duplicates of VMs.

The TOE ensures that any previous information of a snapshot or file is made unavailable upon the deallocation of the resource from user storage (HDD disks and SSD disks).

If a drive error (resulting in the loss of or inability to read user data) occurs, the TOE is able to correct the error on the drive due to RAID 6 technology.

1.5.1.3 Identification and Authentication

The Identification and Authentication function allows the following actions prior to authentication:

- Use of storage services
- Exportation of VMs and vDisks
- Administrative users can access API version information
- Administrative users can access summary performance, alerts, and hardware statistic information

The TOE ensures that the administrative user that is requesting an authenticated service has provided a valid administrative user ID and password and is authorized to access that service.

Administrative users can authenticate to the TOE using either local credentials, or via LDAP. For each administrative user, the TOE stores the administrative user ID, role, and local password security attributes. The Management GUI provides obscured feedback during the authentication process.

1.5.1.4 Security Management

The TOE implements three administrative user roles: Super Admin, Storage Admin, and Read-Only User. Super Admins can perform all management tasks on the system. Storage Admins can perform all management tasks on the system except for managing administrative user accounts. Read-Only Users may only monitor the system, and cannot execute any changes to configurations.

The VM Migration Access Control policy ensures that only authorized administrative users can modify, delete, or create the NFS white list of allowed Host IP addresses via the Management GUI. The VM Migration Access Control policy also enforces a restrictive default NFS white list.

Only authorized administrative users can create, modify, or delete administrative user accounts. The NFS white list, administrative user accounts, exportation services, and snapshot services can all be configured by the TOE.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

1.5.1.5 Protection of the TSF

The appliance contains two storage controllers to provide high availability. The Tintri file system first writes data to non-volatile memory on the active controller and then syncs user data from the active controller to the non-volatile memory on the standby controller to ensure that the file system contents are redundantly stored. This process occurs in less than a millisecond (or a few seconds if a controller is coming back from a failure). Because the user data is synced between two controllers, no data will be lost if there is a controller failure.

The TOE generates timestamps which are included in audit records and used for syncing the two controllers. The TOE ensures the availability and data consistency of configuration data that is provided to another trusted IT[30] product. The TOE runs a suite of self tests during initial start-up to ensure the correct operation of the TOE.

1.5.1.6 Resource Utilization

The TOE's dual-controller architecture and RAID 6 technology ensures the operation of all of the TOE's capabilities in case of a controller or disk failure.

1.5.1.7 TOE Access

The TOE allows administrative users to terminate their own sessions.

1.5.2 Guidance Documentation

The following guides are required reading and part of the TOE:

- 750-5000-6001-Q Tintri VMstore System Administration Manual
- 761-6001-0001-E Tintri VMstore T800 Series Reference Guide
- 765-0301-0201-RevB Tintri VMstore Release Notes
- Tintri, Inc. Tintri VMstore v3.1.2.1 Guidance Documentation Supplement v0.4

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

Additional features/functionality that are not part of the evaluated configuration of the TOE are:

- SSH[31]
- Management Console Access via KVM
- Autosupport
- Tintri VAAI[32] plug-in
- SMTP services
- SNMPv3 services
- NTP[33] services

[30] IT – Information Technology
[31] SSH – Secure Shell
[32] VAAI – vSphere Storage APIs for Array Integration
[33] NTP – Network Time Protocols

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

2 Conformance Claims

This section and Table 2 provide the identification for any CC, Protection Profile (PP), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 8.1.

Table 2 CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012; CC Part 2 extended; CC Part 3 conformant; Parts 2 and 3 Interpretations of the CEM as of 2014/06/06 were reviewed, and no interpretations apply to the claims made in this ST.
PP Identification	None
Evaluation Assurance Level	EAL2+ Augmented with Flaw Remediation (ALC_FLR.2)

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

3 Security Problem

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

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

3.1 Threats to Security

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

- Attackers who are not TOE 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.
- 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. (TOE administrative users are, however, assumed not to be willfully hostile to the TOE.)
- Agents or processes working either on behalf of attackers or autonomously: They may or may not have knowledge of the public or proprietary TOE configuration settings/parameters. These agents and processes can take many forms, such as bots or botnets designed to exploit common vulnerabilities or deny others access to IT products and services.

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 Security Objectives. Table 3 below lists the applicable threats.

Table 3 Threats

Name	Description
T.MASQUERADE	A user or process may masquerade as another entity by sending spoofed IP packets in order to gain access to TOE data path.
T.DATA_AVAILABILITY	TOE data may become unavailable due to isolated storage resource failures, security mechanism failures, or due to resource exhaustion.
T.DATA_TAMPERING	Malicious individuals may take actions to make unauthorized changes to user data or an administrative user may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.UNDETECTED_ACTIONS	Malicious remote individuals or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.

3.2 Organizational Security Policies

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

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 administrative user guidance. Table 4 lists the specific conditions that are required to ensure the security of the TOE and are assumed to exist in an environment where this TOE is employed.

Table 4 Assumptions

Name	Description
A.LOCATE	The TOE is located within a controlled access facility and appropriately located within the network to perform its functions. The connection between the TOE and the target appliance for the exportation of data is also located within a controlled access facility.
A.NOEVIL	The users who manage the TOE are non-hostile, appropriately trained, and follow all guidance.
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or administrative user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.MANAGE	There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.PROTECTED	The TOE is protected from external tampering and interferences.
A.TRUSTED	Only trusted devices will have access to the TOE data path. Users are assumed to be trusted not to spoof the IP address used for accessing the TOE data path.
A.MANAGEMENT_INTERFACE	The TOE is protected from hostile or unauthorized access to the TOE management interface.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

4 Security Objectives

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

4.1 Security Objectives for the TOE

The specific security objectives for the TOE are listed in Table 5 below.

Table 5 Security Objectives for the TOE

Name	Description
O.ACCESS_CONTROL	TOE administrative users will be allowed access to user data if they have an allowed IP address.
O.AVAILABILITY	The TOE will ensure that it can operate securely after a single hardware or software failure.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and provide the means to store and review that data.
O.TIMESTAMP	The TOE will provide a reliable timestamp for use by the TOE.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only authorized administrative users are able to log in and configure the TOE. The TOE also provides the functions necessary to support the administrative users operating the TOE and restricts logged-in administrative users to those authorized functions and TSF data.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.

4.2 Security Objectives for the Operational Environment

This section describes the environmental objectives.

4.2.1 IT Security Objectives

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

Table 6 IT Security Objectives

Name	Description
OE.PROTECT	The TOE environment must protect itself and the TOE from external interference, tampering or physical attacks.
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or administrative user applications) available on the TOE, other than

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description
	those services necessary for the operation, administration and support of the TOE.
OE.SECURE_NETWORK	The Local Area Network that the TOE and TOE environmental components connect to during the exportation of VMs is a secure network that provides protection against outside attacks. The TOE is located on the network behind a secure firewall that protects the TOE against hostile or unauthorized access.
OE.TRUSTED_DEVICES	The TOE environment shall ensure that only trusted devices and users have access to the TOE data path.

4.2.2 Non-IT Security Objectives

Table 7 below lists the non-IT environment security objectives that are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus, they will be satisfied largely through application of procedural or administrative measures.

Table 7 Non-IT Security Objectives

Name	Description
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.
OE.TRUSTED_ADMIN	Sites deploying the TOE will provide competent, non-hostile TOE administrative users who are appropriately trained and follow all administrative user guidance in a trusted manner.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

This section specifies the extended SFRs for the TOE. The extended SFRs are organized by class. Table 8 identifies all extended SFRs implemented by the TOE

Table 8 Extended TOE Security Functional Requirements

Name	Description
FIA_UIA_EXT.1	Administrative User Identification and Authentication
FPT_TST_EXT.1	TSF Testing

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5.1.1 Class FIA: Identification and Authentication

Families in this class address the requirements for functions to establish and verify a claimed administrative user identity as defined in CC Part 2.

5.1.1.1 Family FIA_UIA_EXT: Administrative User Identification and Authentication

Family Behavior

This family defines the types of administrative user identification and authentication mechanisms supported by the TSF.

This section defines the components for the extended FIA_UIA_EXT family, which is modeled after the FIA_UAU and FIA_UID families.

Component Leveling

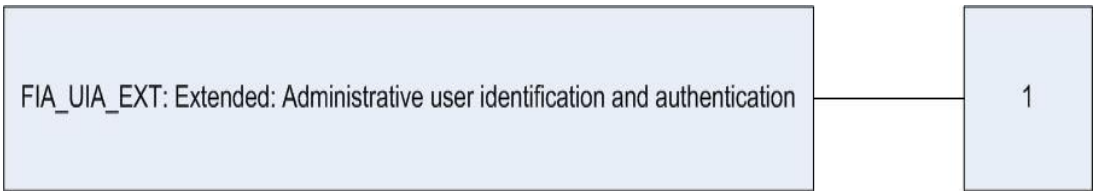

Figure 3 Administrative user identification and authentication family decomposition

FIA_UIA_EXT.1 Extended: Administrative user identification and authentication is the only component of this class, and is modeled after the FIA_UIA_EXT.1 requirement from the Network Device Protection Profile. This component defines the actions available to administrative users prior to initiating the identification and authentication process, and requires administrative users to be successfully identified and authenticated prior to interacting with the TSF.

Management: FIA_UIA_EXT.1

The following actions could be considered for the management functions in FMT:

a) Management of the authentication data by an administrator;
b) Management of the authentication data by the associated administrative user;
c) Managing the list of actions that can be taken before the administrative user is identified and authenticated;
d) Management of the administrative user identities;

Audit: FIA_UIA_EXT.1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a) All use of the identification and authentication mechanism.

FIA_UIA_EXT.1 Administrative user identification and authentication

Hierarchical to: **FIA_UID.1 Timing of identification**
FIA_UAU.1 Timing of Authentication
Dependencies: **No dependencies**

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process:

- [selection: no other actions, [assignment: list of services, actions performed by the TSF in response to non-TOE requests.]]

FIA_UIA_EXT.1.2

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

5.1.2 Class FPT: Protection of the TSF

Families in this class address the requirements for functions providing integrity and management of mechanisms that constitute the TSF and of the TSF data as defined in CC Part 2.

5.1.2.1 Family FPT_TST_EXT: TSF Testing

Family Behavior

Components in this family address the requirements for self-testing the TSF for selected correct operation.

The extended FPT_TST_EXT family is modeled after the FPT_TST family.

Component Leveling

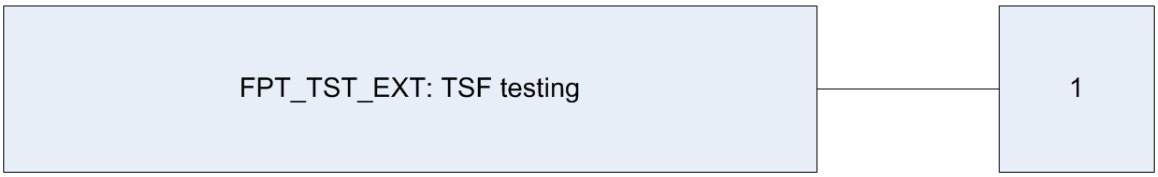

Figure 4 Extended: TSF testing family decomposition

FPT_TST _EXT.1: TSF testing is the only component of this family. This component requires a suite of self tests to be run during initial start-up in order to demonstrate correct operation of the TSF. This requirement is from the Network Device Protection Profile.

Management: FPT_TST _EXT.1

a) There are no management activities foreseen.

Audit: FPT_TST _EXT.1

a) There are no auditable activities foreseen.

FPT_TST_EXT.1 TSF testing

Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_TST_EXT.1.1

The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

5.2 Extended TOE Security Assurance Components

There are no extended SARs defined for this ST.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.
- Extended Functional and Assurance Requirements are identified using "_EXT" at the end of the short name.
- Iterations are identified by appending a letter in parentheses following the component title. For example, FAU_GEN.1(a) Audit Data Generation would be the first iteration and FAU_GEN.1(b) Audit Data Generation would be the second iteration.

6.2 Security Functional Requirements

This section specifies the SFRs for the TOE. This section organizes the SFRs by CC class. Table 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_GEN.2	User identity association				
FAU_SAR.1	Audit review		✓		
FAU_STG.1	Protected audit trail storage	✓			
FAU_STG.4	Prevention of audit data loss	✓	✓		
FDP_ACC.1(a)	Subset access control - VM Migration Access Control Policy		✓		✓
FDP_ACC.1(b)	Subset access control - VM HA Access Control Policy		✓		✓
FDP_ACF.1(a)	Security attribute based access control - VM Migration Access Control Policy		✓		✓
FDP_ACF.1(b)	Security attribute based access control - VM HA Access Control Policy		✓		✓
FDP_ETC.2	Export of user data without security attributes		✓		
FIA_ATD.1	User attribute definition		✓		

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Name	Description	S	A	R	I
FIA_UAU.5	Multiple authentication mechanisms		✓		
FIA_UAU.7	Protected authentication feedback		✓		
FIA_UIA_EXT.1	Administrative user identification and authentication	✓	✓		
FMT_MSA.1	Management of security attributes		✓		
FMT_MSA.3	Static attribute initialization	✓	✓		
FMT_MTD.1	Management of TSF data	✓	✓		
FMT_SMF.1	Specification of management functions		✓		
FMT_SMR.1	Security roles		✓		
FPT_FLS.1	Failure with preservation of secure state		✓		
FPT_STM.1	Reliable time stamps				
FPT_TST_EXT.1	TSF testing				
FRU_FLT.1	Degraded fault tolerance		✓		
FTA_SSL.4	User-initiated termination				

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

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 administrative user actions (except read-only actions)*
- *all debug actions*
- *system errors*

].

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_GEN.2 User identity association
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification
FAU_GEN.2.1

For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAR.1 Audit review
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_SAR.1.1

The TSF shall provide [*administrative users*] 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.

FAU_STG.1 Protected audit trail storage
Hierarchical to: No other components.
Dependencies: FAU_GEN.1 Audit data generation
FAU_STG.1.1

The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2

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

FAU_STG.4 Prevention of audit data loss
Hierarchical to: FAU_STG.3 Action in case of possible audit data loss
Dependencies: FAU_STG.1 Protected audit trail storage
FAU_STG.4.1

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.2 Class FDP: User Data Protection

FDP_ACC.1(a) Subset access control – VM Migration Access Control Policy
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1

The TSF shall enforce the [*VM Migration Access Control Policy*] on [
Subjects:
- *Clients*

Objects:
- *VMstore appliance*

].

FDP_ACC.1(b) Subset access control – VM HA Access Control Policy
Hierarchical to: No other components.
Dependencies: FDP_ACF.1 Security attribute based access control
FDP_ACC.1.1

The TSF shall enforce the [*VM HA Access Control Policy*] on [
Subjects:
- *Initiating VMstore appliance*

Objects:
- *Destination VMstore appliance*

].

FDP_ACF.1(a) Security attribute based access control – VM Migration Access Control Policy
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 [*VM Migration Access Control Policy*] to objects based on the following: [
Subject attributes:
- *Host IP address*

Object attributes:
- *NFS white list*

].
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 process (identified by host IP address) is designated in the NFS white list, 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 [*no other rules*].

FDP_ACF.1(b) Security attribute based access control – VM HA Access Control Policy
Hierarchical to: No other components.
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

FDP_ACF.1.1

The TSF shall enforce the [*VM HA Access Control Policy*] to objects based on the following: [
Subject attributes:

- *Initiating IP address*
- *Authentication key*
- *Destination IP address*

Object attributes:

- *Initiating IP address*
- *Authentication key*
- *Destination IP address*

].

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 initiating VMstore appliance is configured with a valid initiating IP address, authentication key, and destination IP address, access is allowed for exportation services. If any of these attributes do not match what the destination VMstore appliance has on file, 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 [*no other rules*].

FDP_ETC.2 Export of user data with security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

FDP_ETC.2.1

The TSF shall enforce the [*VM HA Access Control Policy*] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2

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

FDP_ETC.2.3

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

FDP_ETC.2.4

The TSF shall enforce the following rules when user data is exported from the TOE: [

1. *The initiating VMstore appliance will initiate the exportation request.*
2. *The TOE must have at least one saved snapshot which will be used to export a copied VM.*
3. *VMs are exported with associated file owner, group owner, and permissions if the initiating IP address, authentication key, and destination IP address match those that are on file in the destination VMstore appliance.*

].

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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: [*Administrative User ID, Role, Password*].

FIA_UAU.5 Multiple authentication mechanisms
Hierarchical to: No other components.
Dependencies: No dependencies.
FIA_UAU.5.1

The TSF shall provide [*Local authentication, LDAP*] to support user authentication.
FIA_UAU.5.2

The TSF shall authenticate any user's claimed identity according to the [*verification of local authentication or by querying a remote authentication server*].

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

The TSF shall provide only [*obscured feedback via the Management GUI*] to the user while the authentication is in progress.

FIA_UIA_EXT.1 Administrative user identification and authentication
Hierarchical to: FIA_UID.1 Timing of identification
FIA_UAU.1 Timing of Authentication
Dependencies: No dependencies
FIA_UIA_EXT.1.1

The TSF shall allow the following actions prior to requiring the non-TOE entity to initiate the identification and authentication process: [

- *Use of storage services*
- *Exportation of VMs and vDisks*
- *Administrative users can access API version information*
- *Administrative users can access summary performance, alerts, and hardware statistic information*

]
FIA_UIA_EXT.1.2

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

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 [*VM Migration Access Control Policy*] to restrict the ability to [modify, delete, *create*] the security attributes [*NFS white list*] to [*an authorized administrative user*].

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components.
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1

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

FMT_MSA.3.2

The TSF shall allow the [*authorized administrative user*] 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 [modify, delete, *create*] the [*administrative user accounts]* to [*the authorized administrative users*].

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components.
Dependencies: No Dependencies

FMT_SMF.1.1

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

- *NFS white list*
- *Administrative user accounts*
- *Exportation services*
- *Snapshot services*

]

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: [*Super Admin, Storage Admin, and Read-Only User*].

FMT_SMR.1.2

The TSF shall be able to associate users with roles.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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: [*controller failure, failure of two disk drives*].

FPT_STM.1 Reliable time stamps
Hierarchical to: No other components.
Dependencies: No dependencies
FPT_STM.1.1

The TSF shall be able to provide reliable time stamps.

FPT_TST_EXT.1 TSF testing
Hierarchical to: No other components.
Dependencies: No dependencies.
FPT_TST_EXT.1.1

The TSF shall run a suite of self tests during initial start-up (on power on) to demonstrate the correct operation of the TSF.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

6.2.6 Class FRU: Resource Utilization

FRU_FLT.1 Degraded fault tolerance
Hierarchical to: No other components.
Dependencies: FPT_FLS.1 Failure with preservation of secure state
FRU_FLT.1.1

The TSF shall ensure the operation of [*all capabilities*] when the following failures occur: [*controller failure, failure of two disk drives*].

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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 the 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[34] 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

[34] CM – Configuration Management

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

7 TOE Security 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_GEN.2	User identity association
	FAU_SAR.1	Audit review
	FAU_STG.1	Protected audit trail storage
	FAU_STG.4	Prevention of audit data loss
User Data Protection	FDP_ACC.1(a)	Subset access control - VM Migration Access Control Policy
	FDP_ACC.1(b)	Subset access control - VM HA Access Control Policy
	FDP_ACF.1(a)	Security attribute based access control - VM Migration Access Control Policy
	FDP_ACF.1(b)	Security attribute based access control - VM HA Access Control Policy
	FDP_ETC.2	Export of user data without security attributes
Identification and Authentication	FIA_ATD.1	User attribute definition
	FIA_UAU.5	Multiple authentication mechanisms
	FIA_UAU.7	Protected authentication feedback
	FIA_UIA_EXT.1	Administrative user identification and authentication
Security Management	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialization
	FMT_MTD.1	Management of TSF data
	FMT_SMF.1	Specification of management functions

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

TOE Security Functionality	SFR ID	Description
	FMT_SMR.1	Security roles
Protection of TOE Security Functions	FPT_FLS.1	Failure with preservation of secure state
	FPT_STM.1	Reliable time stamps
	FPT_TST_EXT.1	TSF testing
Resource Utilization	FRU_FLT.1	Degraded fault tolerance
TOE Access	FTA_SSL.4	User-initiated termination

7.1.1 Security Audit

The TOE records audits for each administrative action on the Management GUI. Auditing begins upon startup of the TOE and does not halt until the TOE is shutdown. The TOE also keeps audit logs for all debug actions and system errors. These audit logs include the data and time of the event, associated administrative user ID, type of the event, and outcome (if applicable). 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.

All administrative users have the capability to read all information from the audit logs. The TOE prevents unauthorized modification or deletion of the stored audit logs in the audit trail; the audit logs can only be overwritten when the audit logs are rotated due to time and capacity.

TOE Security Functional Requirements Satisfied: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_STG.1, FAU_STG.4.

7.1.2 User Data Protection

The TOE implements a VM Migration Access Control Policy to control access to the virtual machines and virtual disks on the storage appliance. Hosts are allowed or denied access via NFS based on whether the host IP address falls within a range of accepted IP addresses stored on the appliance.

The TOE enforces the VM HA Access Control Policy when exporting user data (with associated file owner, group owner, and permissions) when VMs are exported to another VMstore appliance. The exported copies of VMs are created by the TOE using manual, cloned, or scheduled snapshots and cached data.

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

7.1.3 Identification and Authentication

The TOE maintains the administrative user ID, role, and local password attributes belonging to administrative users. Besides local authentication, administrative users can access the Management GUI via remote authentication using LDAP and AD. The TOE verifies the local authentication or queries a remote authentication server to ensure the authentication of an administrative user's claimed identity. Before authentication, administrative users can access API version, summary performance, alerts, and hardware statistic information. Also, the use of the storage services and the exportation of VMs and vDisks occur without authentication.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

When an administrative user logs in to the Management GUI, the Management GUI obscures the feedback while authentication is in process.

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

7.1.4 Security Management

Security management functionality is achieved via the Management GUI. The TOE can be utilized by three different types of roles:

- Super Admin
- Storage Admin
- Read-Only User

The appliance implements a role-based access control policy that defines the privileges for each of the roles. The Super Admin can perform all management tasks on the system. This role includes the ability to create, modify, or delete administrative user ID and password security attributes for administrative users. The Storage Admin performs all management tasks except for managing administrative user accounts, and Read-Only Users can only monitor the system.

The Super Admin can create, modify, or delete the administrative user accounts and manage user data. The Storage Admin can perform the same privileges except for creating, modifying, or deleting administrative user accounts.

The VM Migration Access Control policy enforces a restrictive default NFS white list. Administrative users must configure the allowed IP addresses in the evaluated configuration.

The TOE ensures that only authorized administrative users can create, modify, or delete administrative user accounts. The function is either not presented to an unauthorized administrative user or the action is denied and an error message appears saying that the administrative user has insufficient privileges to perform the attempted task. The NFS white list, administrative user accounts, exportation services, and snapshot services can all be configured by the TOE.

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

The TOE maintains a secure state by continuing to offer all of its functionality in the event of:

- Controller failure
- Failure of two disk drives

This high level of availability is provided through the use of dual-controller architecture. The Tintri file system syncs user data from the NVRAM[35] on the active controller to that on the standby controller, to ensure system contents match. A Fletchum checksum is calculated on the contents of NVRAM on the primary controller as data is synced and verified with the checksum calculated independently by the secondary controller. When the Tintri Operating System receives a write request, data is buffered into the NVRAM device on the primary controller and forwarded to the NVRAM device on the secondary controller. After acknowledgement from the secondary controller that data was safely persisted on its NVRAM, the primary controller acknowledges the write operation. Timestamps are used for synchronization of the controllers.

[35] NVRAM – Non-Volatile Random-Access Memory

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

The Tintri exportation technology allows for VMs to be exported to another VMstore appliance if a replication network has been configured.

Audit logs are kept in internal storage. Timestamps for the audit logs can be gathered from the internal clock on the device.

The SSD and HDD disks are shared by the active and standby controllers, but only one controller can have ownership of at one time. RAID 6 on SSD and HDD provides continuous system operation even when two drives utilized by a controller fail simultaneously. The Tintri RAID 6 software detects and corrects errors in real-time upon every read from the disk. Dual parity is used by RAID 6 to ensure the availability of data when 2 SSD and 2 HDD disks fail. Two parity disks ensure that if one disk fails, there is sufficient data in the remaining disk to reconstruct the missing data.

Self-tests are run at startup to ensure that the TOE is functioning properly. When the appliance is powered on, a system BIOS[36] self-check occurs. After the self-check is completed successfully, the Tintri Operating System begins its boot process. Next, a hardware verification test occurs to ensure that all components detected in the appliance are supported (e.g. SSD and HDD models, NIC[37]s, etc.) and that firmware versions are correct. The TOE also runs tests for the amount of RAM[38], number of disks, and other assembly checks.

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

7.1.6 Resource Utilization

The TOE's dual-controller architecture and RAID 6 technology provides a minimal impact of performance in the event of:

- Controller failure
- Failure of two disk drives

Refer to Section 7.1.5 for more information regarding the RAID 6 technology features that protect the TOE against the failure of two disk drives.

TOE Security Functional Requirements Satisfied: FRU_FLT.1.

7.1.7 TOE Access

The TOE provides the ability for administrative users to terminate their own sessions while accessing the appliance via the Management GUI.

TOE Security Functional Requirements Satisfied: FTA_SSL.4.

[36] BIOS – Basic Input/Output System
[37] NIC – Network Interface Card
[38] RAM – Random-Access Memory

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8 Rationale

8.1 Conformance Claims Rationale

This Security Target conforms to Part 2 and Part 3 of the *Common Criteria for Information Technology Security Evaluation*, Version 3.1 Release 4.

8.2 Security Objectives Rationale

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

8.2.1 Security Objectives Rationale Relating to Threats

Table 12 below provides a mapping of the objects to the threats they counter.

Table 12 Threats: Objectives Mapping

Threats	Objectives	Rationale
T.MASQUERADE A user or process may masquerade as another entity by sending spoofed IP packets in order to gain access to TOE data path.	OE.TRUSTED_DEVICES The TOE environment shall ensure that only trusted devices and users have access to the TOE data path.	OE.TRUSTED_DEVICES mitigates this threat by ensuring that only trusted devices can access the TOE data path.
T.DATA_AVAILABILITY TOE data may become unavailable due to isolated storage resource failures, security mechanism failures, or due to resource exhaustion.	O.AVAILABILITY The TOE will ensure that it can operate securely after a single hardware or software failure.	O.AVAILABILITY mitigates this threat by ensuring that the TOE and its resources are still available when a controller or drive fails.
	O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	O.TSF_SELF_TEST mitigates this threat by ensuring that self-tests are run during the initial self-test to check that the TOE is operating correctly.
T.DATA_TAMPERING Malicious individuals may take actions to make unauthorized changes to user data or an administrative user may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.	O.ACCESS_CONTROL TOE administrative users will be allowed access to user data if they have an allowed IP address.	O.ACCESS_CONTROL mitigates this threat by ensuring that only authorized administrative users can access user data.
	O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only authorized administrative users are able to log in and configure the TOE. The TOE also provides the functions necessary to support the administrative users operating the TOE and restricts logged-in administrative users to those authorized functions and TSF data.	O.TOE_ADMINISTRATION mitigates this threat by ensuring that only authorized administrative users are able to log in and configure the TOE and that logged in administrative users are restricted to authorized functions and TSF data.
T.UNDETECTED_ACTIONS	O.SYSTEM_MONITORING	O.SYSTEM_MONITORING

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Threats	Objectives	Rationale
Malicious remote individuals or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.	The TOE will provide the capability to generate audit data and provide the means to store and review that data.	mitigates this threat by ensuring that all administrative user actions will be present in the TOE's audit records.
	O.TIMESTAMP The TOE will provide a reliable timestamp for use by the TOE.	O.TIMESTAMP mitigates this threat by ensuring that all security-related activity on the TOE is audited and recorded with the time that the actions were performed.

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

Table 13 Assumptions: Objectives Mapping

Assumptions	Objectives	Rationale
A.LOCATE The TOE is located within a controlled access facility and appropriately located within the network to perform its functions. The connection between the TOE and the target appliance for the exportation of data is also located within a controlled access facility.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference, tampering or physical attacks.	OE.PROTECT satisfies this assumption by ensuring that the environment provides protection against external interference, tampering or physical attacks.
	OE.SECURE_NETWORK The Local Area Network that the TOE and TOE environmental components connect to during the exportation of VMs is a secure network that provides protection against outside attacks. The TOE is located on the network behind a secure firewall that protects the TOE against hostile or unauthorized access.	OE.SECURE_NETWORK satisfies the assumption by ensuring that the TOE and TOE environmental components connected to the Local Area Network are protected from outside attacks.
A.NO_GENERAL_PURPOSE It is assumed that there are no general-purpose computing capabilities (e.g., compilers or administrative user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE There are no general-purpose computing capabilities (e.g., compilers or administrative user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.	OE.NO_GENERAL_PURPOSE satisfies the assumption by ensuring that there are no general-purpose computing capabilities available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.PHYSICAL	OE.PHYSICAL	OE.PHYSICAL satisfies this

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Assumptions	Objectives	Rationale
Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.	Physical security, commensurate with the value of the TOE and the data it contains, is provided by the environment.	assumption that physical security is provided within the TOE environment to provide appropriate protection to the network resources.
A.MANAGE There are one or more competent individuals assigned to manage the TOE and the security of the information it contains.	OE.TRUSTED_ADMIN Sites deploying the TOE will provide competent, non-hostile TOE administrative users who are appropriately trained and follow all administrative user guidance in a trusted manner.	OE.TRUSTED_ADMIN satisfies the assumption that competent individuals are assigned to manage the TOE and the TSF and to follow guidance in a trusted manner.
A.PROTECTED The TOE is protected from external tampering and interferences.	OE.PROTECT The TOE environment must protect itself and the TOE from external interference, tampering or physical attacks.	OE.PROTECT satisfies the assumption that the TOE will be protected from unauthorized tampering or interference.
A.TRUSTED Only trusted devices will have access to the TOE data path. Users are assumed to be trusted not to spoof the IP address used for accessing the TOE data path.	OE.TRUSTED_DEVICES The TOE environment shall ensure that only trusted devices and users have access to the TOE data path.	OE.TRUSTED_DEVICES satisfies the assumption by ensuring that only trusted devices and users will have access to the TOE data path.
A.MANAGEMENT_INTERFACE The TOE is protected from hostile or unauthorized access to the TOE management interface.	OE.SECURE_NETWORK The Local Area Network that the TOE and TOE environmental components connect to during the exportation of VMs is a secure network that provides protection against outside attacks. The TOE is located on the network behind a secure firewall that protects the TOE against hostile or unauthorized access.	OE.SECURE_NETWORK satisfies the assumption that the TOE will be protected from hostile or unauthorized access to the TOE management network by ensuring that the TOE is located on the network behind a secure firewall.

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

The TOE contains the following explicitly stated security functional requirements:

- FIA_UIA_EXT.1
- FPT_TST_EXT.1

FPT_UIA_EXT is an explicitly-stated functional requirement modeled on the FPT_UIA_EXT requirement from the Network Device Protection Profile. The SFR family "Administrative user identification and authentication" was created to specifically address the timing of identification and authentication. The SFR

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

in this family has no dependencies since the stated requirement embodies all necessary security functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

FPT_TST_EXT is an explicitly-stated functional requirement from the Network Device Protection Profile. The SFR family "TSF testing" was created to ensure that a suite of self tests are run to demonstrate the correct operation of the TSF. The SFR in this family has no dependencies since the stated requirement embodies all necessary security functions. This requirement exhibits functionality that can be easily documented in the ADV assurance evidence and thus do not require any additional Assurance Documentation.

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 14 below shows a mapping of the objectives and the SFRs that support them.

Table 14 Objectives: SFRs Mapping

Objective	Requirements Addressing the Objective	Rationale
O.ACCESS_CONTROL TOE administrative users will be allowed access to user data if they have an allowed IP address.	FDP_ACC.1(a) Subset access control - VM Migration Access Control Policy	The requirement meets the objective by ensuring that the TOE enforces an access control SFP for a subset of the possible operations on a subset of the objects in the TOE.
	FDP_ACC.1(b) Subset access control - VM HA Access Control Policy	The requirement meets the objective by ensuring that the TOE enforces an access control SFP for a subset of the possible operations on a subset of the objects in the TOE.
	FDP_ACF.1(a) Security attribute based access control - VM Migration Access Control Policy	The requirement meets the objective by defining the security attributes on which the enforced access control TSF is based on.
	FDP_ACF.1(b) Security attribute based access control - VM HA Access Control Policy	The requirement meets the objective by defining the security attributes on which the enforced access control TSF is based on.
	FMT_MSA.1 Management of security attributes	The requirement meets the objective by ensuring that the

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
		TOE enforces the access control SFP regarding the management of security attributes.
	FMT_MSA.3 Static attribute initialization	The requirement meets the objective by ensuring that the TOE enforces the access control SFP to ensure that only authorized administrative users can override default values.
O.AVAILABILITY The TOE will ensure that it can operate securely after a single hardware or software failure.	FDP_ETC.2 Export of user data without security attributes	The requirement meets the objective by ensuring the availability of user data by exporting VMs to another VMstore appliance.
	FPT_FLS.1 Failure with preservation of secure state	The requirement meets the objective by ensuring that the TOE maintains a secure state in the event of controller or drive failures.
	FRU_FLT.1 Degraded fault tolerance	The requirement meets the objective by ensuring that all of the TOE's capabilities are available when a drive or controller error occurs.
O.SYSTEM_MONITORING The TOE will provide the capability to generate audit data and provide the means to store and review that data.	FAU_GEN.1 Audit data generation	The requirement meets this objective by ensuring that the TOE maintains a record of defined security related events, including relevant details about the event.
	FAU_GEN.2 User identity association	The requirement meets this objective by ensuring that the TOE associates an administrative user with the audit records.
	FAU_SAR.1 Audit review	The requirement meets the objective by ensuring that the TOE provides the ability to review logs.
	FAU_STG.1 Protected audit trail storage	The requirement meets the objective by ensuring that the TOE protects the audit data from unauthorized deletion.
	FAU_STG.4 Prevention of audit data loss	If the audit facilities become full, the TOE ensures that only the oldest records are overwritten. This requirement meets this objective by mitigating the risk of loss of audit trail data.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Objective	Requirements Addressing the Objective	Rationale
O.TIMESTAMP The TOE will provide a reliable timestamp for use by the TOE.	FPT_STM.1 Reliable time stamps	The requirement meets the objective by ensuring that the TOE provides reliable timestamps.
O.TOE_ADMINISTRATION The TOE will provide mechanisms to ensure that only authorized administrative users are able to log in and configure the TOE. The TOE also provides the functions necessary to support the administrative users operating the TOE and restricts logged-in administrative users to those authorized functions and TSF data.	FIA_ATD.1 User attribute definition	The requirement meets the objective by defining the list of security attributes belonging to the administrative users.
	FIA_UAU.5 Multiple authentication mechanisms	The requirement meets the objective by defining the multiple authentication mechanisms and its rules.
	FIA_UAU.7 Protected authentication feedback	The requirement meets the objective by ensuring that the TOE provides obscured feedback while authentication is in progress.
	FIA_UIA_EXT.1 Administrative user identification and authentication	The requirement meets the objective by defining the list of actions or services that can be performed before identification and authentication.
	FMT_MTD.1 Management of TSF data	The requirement meets the objective by ensuring that the TOE restricts the management of TSF data to authorized administrative users.
	FMT_SMF.1 Specification of management functions	The requirement meets the objective by defining the list of management functions that can be performed by the TOE.
	FMT_SMR.1 Security roles	The requirement meets the objective by defining the authorized roles of the TOE.
	FTA_SSL.4 User-initiated termination	The requirement meets the objective by ensuring that the TOE allows an administrative user-initiated termination of the administrative user's own session.
O.TSF_SELF_TEST The TOE will provide the capability to test some subset of its security functionality to ensure it is operating properly.	FPT_TST_EXT.1 TSF testing	The requirement meets the objective by ensuring that the TOE performs a suite of self-tests during initial start-up to demonstrate the correct operation of the security function.

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

8.5.2 Security Assurance Requirements Rationale

EAL2+ was chosen to provide a low to moderate level of assurance that is consistent with good commercial practices. As such, minimal additional tasks are placed upon the vendor assuming the vendor follows reasonable software engineering practices and can provide support to the evaluation for design and testing efforts. The chosen assurance level is appropriate with the threats defined for the environment. The TOE is expected to be in a non-hostile position and embedded in or protected by other products designed to address threats that correspond with the intended environment. At EAL2+, the 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 15 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 15 Functional Requirements Dependencies

SFR ID	Dependencies	Dependency Met	Rationale
FAU_GEN.1	FPT_STM.1	✓	
FAU_GEN.2	FAU_GEN.1	✓	
	FIA_UIA_EXT.1	✓	Although FIA_UID.1 is not claimed, the dependency SFR is substituted by FIA_UIA.1 which is an extension of the combination FIA_UID.1 and FIA_UAU.1.
FAU_SAR.1	FAU_GEN.1	✓	
FAU_STG.1	FAU_GEN.1	✓	
FAU_STG.4	FAU_STG.1	✓	
FDP_ACC.1(a)	FDP_ACF.1	✓	
FDP_ACC.1(b)	FDP_ACF.1	✓	
FDP_ACF.1(a)	FDP_ACC.1	✓	
FDP_ACF.1(b)	FMT_MSA.3	✓	
	FDP_ACC.1	✓	
FDP_ETC.2	FDP_ACC.1	✓	
FIA_ATD.1	No dependencies	Not applicable	
FIA_UAU.5	No dependencies	Not applicable	
FIA_UAU.7	FIA_UIA_EXT.1	✓	Although FIA_UAU.1 is not claimed, the dependency SFR is

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

SFR ID	Dependencies	Dependency Met	Rationale
			substituted by FIA_UIA.1 which is an extension of the combination FIA_UID.1 and FIA_UAU.1.
FIA_UIA_EXT.1	No dependencies	Not applicable	
FMT_MSA.1	FDP_ACC.1	✓	
	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_MSA.3	FMT_MSA.1	✓	
	FMT_SMR.1	✓	
FMT_MTD.1	FMT_SMF.1	✓	
	FMT_SMR.1	✓	
FMT_SMF.1	No dependencies	Not applicable	
FMT_SMR.1	FIA_UIA_EXT.1	✓	Although FIA_UID.1 is not claimed, the dependency SFR is substituted by FIA_UIA.1 which is an extension of the combination FIA_UID.1 and FIA_UAU.1.
FPT_FLS.1	No dependencies	Not applicable	
FPT_STM.1	No dependencies	Not applicable	
FPT_TST_EXT.1	No dependencies	Not applicable	
FRU_FLT.1	FPT_FLS.1	✓	
FTA_SSL.4	No dependencies	Not applicable	

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

9 Acronyms

This section and Table 16 define the acronyms used throughout this document.

9.1 Acronyms

Table 16 Acronyms

Acronym	Definition
AC	Alternating Current
API	Application Programming Interface
BIOS	Basic Input/Output System
CC	Common Criteria
CM	Configuration Management
EAL	Evaluation Assurance Level
G	Gigabit
GbE	Gigabit Ethernet
GUI	Graphical User Interface
HDD	Hard-Disk Drives
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IEC	International Electrotechnical Commission
I/O	Input/Output
IOPS	Input/Output Operations Per Second
IP	Internet Protocol
IT	Information Technology
KVM	Keyboard, Video, Mouse
LDAP	Lightweight Directory Access Protocol
NEMA	National Electrical Manufacturers Association
NFS	Network File System
NIC	Network Interface Card
NTP	Network Time Protocol
NVRAM	Non-Volatile Random-Access Memory
PP	Protection Profile
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RAM	Random-Access Memory

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

Acronym	Definition
REST	Representational State Transfer
RHEV	Red Hat Enterprise Virtualization
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SMTP	Simple Mail Transfer Protocol
SNMPv3	Simple Network Management Protocol Version 3
SSD	Solid-State Drives
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
U	Unit
USB	Universal Serial Bus
V	Volts
VAAI	vSphere Storage APIs for Array Integration
vDisk	Virtual Disk
VM	Virtual Machine

© 2015 Tintri, Inc.
This document may be freely reproduced and distributed whole and intact including this copyright notice.

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