Huawei FusionSphere 5.0 Security Target

Version: 1.0

Last Update: 2015-06-30

Author: Huawei Technologies Co., Ltd.

Revision Record

Date	Revision Version	Description	Author
2015-06-30	1.0	Revised TOE Version	Huhongshan
2015-05-14	0.9	1/Update version of guidance	Huhonghsan
2015-03-03	0.8	1/Remove HA	Huhonghsan
2015-01-31	0.7	1/Assume the OS and OSS are trusted.	Huhonghsan
2015-01-08	0.6	1/Update to R5	Huhonghsan
2014-11-18	0.5	Update based on CC evaluation. Modify: 1/delete firewall as environment component 2/provide detail document list 3/delete comment which confirmed 4/delete information about VM HA	Huhonghsan
2014-10-16	0.4	Updated based on CC evaluation Add: 1/Memory balloon security 2/FireWall as environment component	Hu Hongshan
2014-07-29	0.3	Updated based on CC evaluation	Hu Hongshan
2014-01-20	0.2	Updated based on review comments.	Hu Hongshan Wang Xianlei
2013-12-15	0.1	Initial Draft	Hu Hongshan

Table of Contents

List of Tables

List of Figures

1 Introduction

This Security Target is for the evaluation of Huawei FusionSphere 5.0.

1.1 Security Target Identification

Name: Huawei FusionSphere Security Target

Version: 1.0

Publication Date: 2015-06-30

Author: Huawei Technologies Co., Ltd.

1.2 TOE Identification

Name: Huawei FusionSphere software

Version: 5.0

Sponsor: Huawei

Developer: Huawei

Keywords: Huawei, FusionSphere, Cloud OS

1.3 TOE Overview

The Target of Evaluation (TOE) type is a software system that can provide multiple VMs on industry standard x86-compatible hardware platforms (64-bit) and allows the management of these virtual machines (VMs). It virtualizes hardware resources so that one physical server can function as multiple virtual servers. It consolidates existing workloads on servers and allows new applications and solutions to be deployed to improve server utilization and consolidation ratio.

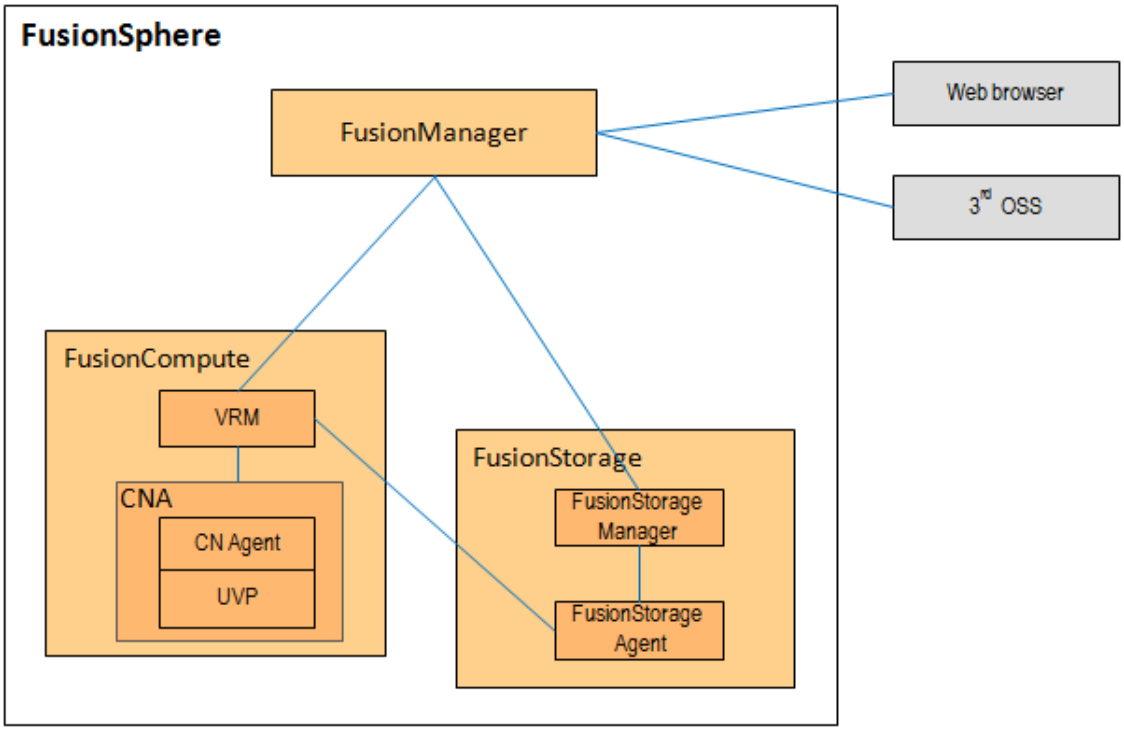
The TOE provides a unified O&M portal for O&M engineers. O&M engineers can remotely access the FusionSphere system using a web browser and perform operations such as resource management, resource monitoring, and resource statistics reporting.

The structure of the TOE is described in section 1.4TOE Description.

1.4 TOE Description

1.4.1 Architecture Overview

Figure 1: TOE architecture



The TOE consists of FusionCompute, FusionManager, and FusionStorage. FusionCompute virtualizes hardware resources and manages and schedules virtual resources. FusionManager manages physical and virtual resources across clusters and data centers in a unified manner. FusionStorage consolidates local hard disks of servers and forms a virtual storage resource pool to provide block storage resources for VMs.

Component	**Function Description**
FusionCompute	FusionCompute is a cloud operating system (OS). It hardware resources and centrally manages virtual resources, services, and users. FusionCompute uses computing, and network virtualization technologies to virtualize hardware computing, storage, and network resources and centrally manages and schedules the virtual resources using a unified portal. FusionCompute consists of the Virtualization Resource Management (VRM) and Computing Node Agent (CNA) nodes.
VRM	Each VRM is a FusionCompute site that contains independent computing, storage, and network resources. VRM allows computing, storage, and network resources to be flexibly

Component	**Function Description**
	configured to meet requirements of different application scenarios.
CNA	A CNA controls computing, storage, and network resources each virtual node(UVP) and functions as an operation and maintenance (O&M) agent(CN Agent). Huawei Universal Virtualization Platform (UVP) that provides the computing, storage, and network technologies must be installed on each CNA. For details, see UVP information below.
FusionManager	FusionManager is a cloud management system that enables administrators to centrally schedule and manage virtual computing, storage, and network resources using a unified portal. FusionManager provides the following functions: • User and rights management • User authentication • Logging and auditing • System management • Monitoring and alarm management • Resource management
FusionStorage	FusionStorage is distributed storage software. After installed on x86 servers, the software can consolidate local hard disks of the servers and form a virtual storage resource pool to provide block storage resources. FusionStorage consists of the FusionStorage Manager and FusionStorage Agent.
FusionStorage Manager	The management module of the FusionStorage system. It supports O&M functions including alarm management, service monitoring, operation logging, and data configuration.
FusionStorage	The agent process of the FusionStorage system.

Component	**Function Description**
Agent	It is deployed on each node or server and communicates with the FusionStorage Manager.

Table 1: FusionSphere components and their functions

1.4.2 UVP Architecture

Configured between the hardware and the OS, the UVP provides virtualized hardware resources for the OS running at the upper layer, manages and allocates resources, and ensures that the upper-layer VMs are isolated from one another.

The UVP has a privileged domain called Domain 0 and some unprivileged domains called Domain U. Domain 0 manages all unprivileged domains and provides virtual resource services.

Figure 2 shows the logical architecture of the UVP.

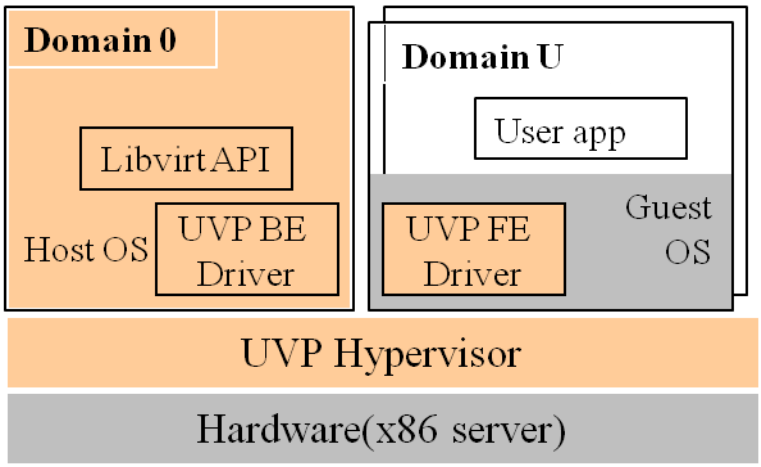


Figure 2: UVP logic architecture

The UVP provides an abstract layer for domains. Application programming interface (APIs) for management and virtual hardware are also included at the layer. UVP Driver (BE Driver) in Domain0 parses disk and network I/O requests from the front-end driver (FE Driver) in DomainU and maps to the actual physical device through native driver. Native driver directly access to physical hardware. UVP Libvirt provides programming interfaces(APIs) for upper layer virtualization resource management.

VMs usually have different software installed and process various data. Therefore, in addition to the security policies provided by VM OS (guest OS), the UVP must also have related policies to ensure the security of VM running environments. One of the most important technologies provided by the UVP for VM security is resource isolation among all domains. This technology ensures that a process running on a VM can access resources on another VM only after being authorized. The UVP implements resource isolation at the following levels to ensure VM security:

1) CPU resources: The UVP properly allocates physical CPU resources to VMs based on optimal scheduling algorithms, such as credit.

2) Physical memory resources: Memory is managed based on partitions. Virtual memory space used by each VM has one-to-one mapping with the physical memory space. The virtualization layer manages the mapping. VMs cannot access the memory of other VMs in an authorized way, thereby implementing VM memory isolation.

3) Devices: The virtualization layer captures all physical device interrupts and forwards the interrupts to VMs. All device interrupts will be forwarded to Domain 0 (a privileged VM) that controls VMs' access to physical devices, thereby isolating VM I/O data.

4) Networks: vSwitch is used to implement centralized network management. Security domains are isolated using the virtual local area network (VLAN) and security groups. All VM network packets must pass through the Domain 0 network bridge. Rules can be added to the iptables of Domain 0 to implement firewall functions.

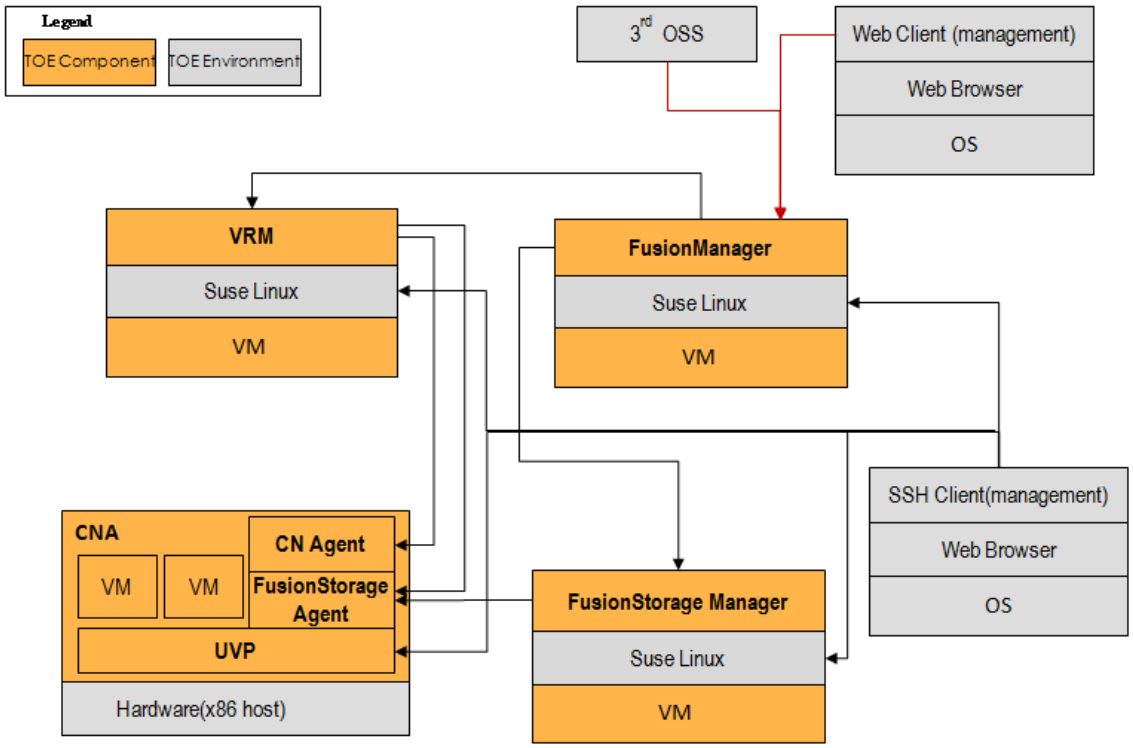
5) VMs: Resource quotas can be configured for each VM to ensure that each VM has an independent running environment.

1.4.3 Physical Scope

This section describes the physical components of the TOE included in this evaluation.

The TOE is a virtualization and management software deployed on x86-compatible servers. This evaluation does not involve hardware and third-party OSs. The servers, storage devices, physical switches, firewalls, OSs, and databases used in this evaluation are TOE environment and meet the security requirements.

Figure 3: TOE physical scope



FusionSphere software packages are binary compressed files. The following software packages and documents are required and are part of the TOE:

Table 2: TOE software and guidance list

Type	Name	Version
Software	FusionCompute VRM	V100R005C00CP3002
	FusionCompute CNA	V100R005C00CP3002
	FusionCompute Tools	V100R005C00SPC300
	FusionManager	V100R005C00SPC302
	FusionStorage Manager	V100R003C02SPC301
	FusionStorage Agent	V100R003C02SPC301
Guidance	FusionSphere Solution Documentation	V100R005C00

	FusionSphere Preparative Procedures	V100R005C00 Issue 02
	FusionSphere Operational User Guidance	V100R005C00 Issue 03
	FusionManager Product Documentation	V100R005C00
	FusionManager Tenant Guide	V100R005C00
	FusionManager Administrator Guide	V100R005C00
	FusionManager Software Installation Guide	V100R005C00
	FusionCompute Product Documentation	V100R005C00
	FusionCompute Security Guide	V100R005C00
	FusionCompute Configuration Management Guide	V100R005C00
	FusionStorage Product Documentation	V100R003C02

Table 3 lists components of the TOE that are included in the TOE scope.

Table 3: TOE components

Component	TOE	TOE Environment
FusionCompute V100R005C00CP3002	✓	
FusionManager V100R005C00SPC302	✓	
FusionStorage V100R003C02SPC301	✓	
NTP server		✓
X86 server		✓

Suse Linux 11 (for VRM/FusionManager/ FusionStorage Manager)		✓
Other OS (such as Windows 7) for user VM		✓
Management terminal hardware and operating system		✓

1.4.4 Non-TOE Hardware/Software/Firmware Required by the TOE

Ensure that the PC, servers, storage devices, and networks meet FusionSphere installation requirements.

1.4.3.1 Management terminal

A PC is required for FusionSphere software installation and initial configuration. **Table 4** lists the PC requirements.

Table 4: PC requirements

Item	Requirements
OS	Windows 7 32-bit
Hard disk space	The partition for installing the OS has more than 30 GB of free space.
Application software	Internet Explorer 8.0 or 9.0, or Mozilla Firefox 12 to 24 If the Mozilla Firefox browser is to be used, Mozilla Firefox 24 is recommended.
Network	The PC used for deploying FusionManager and the server on which FusionManager is to be deployed are connected to the same switch. Both the PC and the server are assigned available management IP addresses. The firewall on the PC is disabled

1.4.3.2 Host

Table 5 lists the host requirements.

Table 5: Host requirements

Item	Requirements
CPU	Intel x86 CPU The CPU supports hardware virtualization technology, such as Intel VT-x, and the CPU virtualization function must be enabled in the BIOS system.
Memory	• Minimum memory size: 8 GB • Recommended memory size > 48 GB
Hard disk	Hard disk size ≥ 16 GB
Network port	• Number of network ports ≥ 1 • Recommended number of network ports: 6 • Recommended network port rate > 1000 Mbit/s
Redundant array of independent disks (RAID)	Configure hard disks 1 and 2 as RAID 1 for installing the host OS to improve storage reliability. When setting the boot device in the host BIOS, set the first boot device to a RAID 1 disk.

1.4.3.3 Management node requirement

Table 6 lists requirements for the VM on which the VRM node is to be deployed.

Table 6: VRM VM requirements

Item	Requirements
Hardware specifications	CPU: At least 2 cores Memory ≥ 4 GB Disk ≥ 80 GB Number of NICs ≥ 1
OS	Novell SUSE Linux Enterprise Server11 SP1 64-bit
Network	The VRM VM must connect to the distributed virtual switch (DVS) and the port group of the management plane.
VM blue screen of death (BSOD)	Select **No processing**.
Clock sync	It is recommended that a precise clock source is configured and

Item	Requirements
	FusionManager is set to synchronize time with the time source. When creating a FusionManager VM on the FusionCompute portal, do not select **Sync time with host**.

Table 7 lists requirements for the VM on which FusionManager is to be deployed.

Table 7: FusionManager VM requirements

Item	Requirements
Hardware specifications	CPU: At least 2 Memory ≥ 4 GB Disk ≥ 80 GB Number of NICs ≥ 1
OS	Novell SUSE Linux Enterprise Server11 SP1 64–bit
Network	The FusionManager VM must connect to the distributed virtual switch (DVS) and the port group of the management plane.
VM blue screen of death (BSOD)	Select **No processing**.
Clock sync	It is recommended that a precise clock source is configured and FusionManager is set to synchronize time with the time source.

1.4.3.4 Storage device requirements

FusionStorage can be installed on Huawei Tecal RH2288, Huawei Tecal E9000, or third-party servers. FusionStorage has the following requirements on the hardware platform on which it is running:

- The servers must be common x86-compatible servers.
- A minimum of three servers are required because FusionStorage uses the distributed cluster architecture.

- The number of hard disks on each server in the cluster must be the same. Four to twelve hard disks can be configured on each server.
- A 4 GB NVDIMM or a PCIe SSD card (400 GB, 800 GB, 1.2 TB, or 2.4 TB) must be configured for each server to ensure that metadata and cache data of FusionStorage will not lose in the event of a power outage.
- Memory used for the running of FusionStorage = 4.7 GB + 1.7 GB x *N* (*N* is the number of hard disks on each server and ranges from 4 to 12). The memory size actually configured for each server must be greater than the value calculated using this formula because some memory needs to be allocated to the OS and applications.
- At least two network ports on each server must be connected to both the management and storage planes. The bandwidth of the storage plane must be greater than or equal to 10 Gbit/s.

1.4.3.5 Network requirements

Communication Plane	Description	Requirement
Baseboard management controller (BMC) plane	Specifies the plane used by the BMC network port on the host. This plane enables remote access to the BMC system on a server.	The management plane of the VRM can communicate with the BMC plane. The management plane and the BMC plane can be combined.
Management plane	Specifies the plane used by the management system that manages all nodes in a unified manner. All nodes communicate with one another on this plane: The management plane provides the following IP addresses:	The VRM can communicate with all CNAs on the management plane.

Communication Plane	Description	Requirement
	• Host management IP addresses (IP addresses used by the management network ports on hosts) • IP addresses of VMs on which management nodes are deployed • IP addresses of storage device controllers You are advised to configure the eth0 on a host as the management network port. If a host has more than four network ports, you are advised to configure both eth0 and eth1 on the host as the management network ports, and bind them after FusionCompute is installed so that they can work in active/standby mode.	
Storage plane	Specifies the plane on which hosts communicate with storage devices. The storage plane provides the following IP addresses: • Host storage IP addresses (IP addresses of the storage network ports on hosts) • Storage IP addresses of storage devices. If the multipathing mode is used, multiple VLANs must be configured for the storage plane.	The hosts can communicate with the storage devices on the storage plane.

Communication Plane	Description	Requirement
Service plane	Specifies the plane used by user VMs on which services are deployed.	The VRM can communicate with the hosts on the service plane if the VRM needs to assign IP addresses to NICs on the service plane.

Huawei FusionSphere need to deploy firewall to protect communication security between management terminal and management plane, and between different communication plane.

1.4.5 Logical Scope

The TOE is a software system that can provide multiple VMs on industry standard x86-compatible hardware platforms (64-bit) and allows the management of these VMs. The major security features implemented by the TOE and subject to evaluation are:

- Authentication

Operators using local and remote access to the TOE in order to execute device management functions are identified by individual user names and authenticated by passwords.

- Access control

Huawei FusionSphere software implements role-based access control, limiting access to different management functions to different roles as defined in administrator-defined access control associations. FusionSphere also ensures that only specific client IP addresses can be used to remotely access the management interface.

- Security audit

Audit records are created for security-relevant events related to the use of FusionSphere.

- Communications security

FusionSphere offers SSL/TLS channels for HTTP access to the management portal.

- Security function management

The TOE offers management functionality for its security functionality.

- VM domain isolation

The hypervisor isolates VMs running on the same physical server to prevent data theft and malicious attacks. VM users can only access resources (hardware and software resources and data) belonging to their own VMs.

- VM Network Separation

Huawei FusionSphere supports virtual switches and VLANs. VMs can be separated by VLAN. Administrators can configure network isolation policies on the management portal.

2 CC Conformance Claim

This ST is CC Part 2 conformant and CC Part 3 conformant. The CC version of [CC] is 3.1R4.

This ST is EAL3 conformant as defined in [CC] Part 3, with the assurance level of EAL3 Augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

3 TOE Security Problem Definition

3.1 Threats

The **information assets** to be protected are the information stored, processed or generated by the TOE. Configuration data for the TOE, TSF data (such as user account information, passwords, and audit records) and other information that the TOE facilitates access to (such as system software, patches and network traffic routed by the TOE) are all considered part of information assets.

Table 8: Threats

Threat Name	Threat Definition
T.NOIDENTIFY	A user who is not a user of the TOE gains access to the TOE.
T.NOAUTH	A user of the TOE authorized to perform certain actions and access certain information gains access to function or information he is not authorized to access.
T. EAVESDROP	An eavesdropper from the management network served by the TOE is able to intercept, and potentially modify or re-use the data that is being sent to the TOE.
T.VM_DOM_BYPASS	A process running on one virtual machine might compromise the security of processes running on that and other virtual machines and its resources.
T.HOST_DOM_BYPASS	An individual may compromise the physical machine processes and resources, potentially affecting other VMs.
T.VNETWORK_BYPASS	An individual may access a virtual network belonging to VMs that do not belong to such individual.

3.2 Assumptions

Table 9 lists the assumptions that are upheld for the operational environment of the TOE.

Table 9: TOE Assumption

Assumption Name	Assumption Definition
A.ADMIN_NO_EVIL	The authorized administrators (including northbound interface users) are not careless, willfully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OS users are trusted and will not attack the TOE.
A.SEP_PHY_NETWORK	It is assumed that the ETH interface of management and storage plane in the TOE will be accessed only through an independent local network. This network is separate from the networks that use the other interfaces of the TOE. The FusionManager manages the NEs through the internal management network plane. It is assumed that the internal management network is secure and the NEs are trusted.
A.PHY_PROPECT	It is assumed that the TOE is protected against unauthorized physical access. Unauthorized users cannot gain access to these devices or components.
A.TIME_SRC	Reliable time stamps for the generation of audit records.
A.OS_TRUESTED	It is assumed that the OSs for FusionManager, FusionStorage Manager and VRM are trusted and the third party OSS is trusted.

4 Security Objectives

4.1 Security objectives for the TOE

Table 10: Security Objectives for the TOE

TOE Security Obj.	Definition
O.Authentication	The TOE must authenticate users before allowing them access to its management interface.
O. Authorization	The TOE shall allow different authorization levels to be assigned to administrators in order to restrict the functionality that is available to individual administrators.
O. Communication	The TOE shall provide a secure remote communication channel for remote administration of the TOE via SSL.
O.Audit	The TOE must be able to generate and review audit records for security-relevant events.
O.VM_DOM_ISO	The TOE must provide virtual machines with a domain of execution and resources protection from interference and tampering by other virtual machines running the same physical host.
O.VNETWORK_ISO	The TOE must maintain virtual networks used for VMs isolated from each other.

4.2 Security Objectives for the Operational Environment

Table 11: Security Objectives for the Operational Environment

Environment Security Objective	Definition
OE.PHY_PROTECTION	The operational environment shall protect the TOE against unauthorized physical access.
OE.SEP_PHY_NETWORK	The operational environment shall ensure that hat the ETH interface in the TOE will be accessed only through an independent local network. This network is separate from

	the networks that use the other interfaces of the TOE. The operational environment shall ensure that the internal management network is secure and the NEs are trusted.
OE.TRUST_WORTHY_USER	Personnel working as authorized administrators (including northbound interface users) shall be carefully selected for trustworthiness and trained for proper operation of the TOE.
OE.TIME_SRC	The operational environment shall provide reliable time source.
OE.OS_TRUSTED	The operational environment shall ensure the OSs for FusionManager, FusionStorage Manager and VRM are trusted and the third party OSS is trusted and will not be used to attack the TOE.

4.3 Security Objectives Rationale

Table 12: Rationale for threats

Threat	Rationale for security objectives to remove threats
T.NOIDENTIFY	The threat of unauthenticated access to the TOE is countered by requiring the TOE to implement an authentication mechanism for its users (O.Authentication). In addition, login attempts are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.NOAUTH	The threat of unauthorized access is countered by requiring the TOE to implement an access control mechanism (O.Authorization). In addition, actions are logged allowing detection of attempts and possibly tracing of culprits (O.Audit)
T.EAVESDROP	The threat of eavesdropping is countered by requiring communications security via SSL for communication between management console and the TOE. (O.Communication).

T.VM_DOM_BYPASS	The threat of VM information theft by other VMs is countered by requiring that information about one VM is invisible to other VMs. (O.VM_DOM_ISO).
T.VNETWORK_BYPASS	The threat of broadcast attacks is countered by requiring that VM packets can only be broadcasted to target interfaces. (O.VNETWORK_ISO).

Table 13: Rationale for assumptions

Assumption	Rationale for security objectives
A.PHY_PROPECT	Directly covered by OE.PHY_PROPECT.
A.SEP_PHY_NETWORK	Directly covered by OE.SEP_PHY_NETWORK.
A. ADMIN_NO_EVIL	Directly covered by OE.TRUST_WORTHY_USER.
A.TIME_SRC	Directly covered by OE. TIME_SRC.
A.OS_TRUSTED	Directly covered by OE.OS_TRUSTED

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 Conventions

The following conventions are used for the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement
- (underlined text in parentheses) indicates additional text provided as a refinement.
- **Bold text** indicates the completion of an assignment.
- ***Italicised and bold text*** indicates the completion of a selection.
- Iteration/N indicates an element of the iteration, where N is the iteration number/character.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

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) **[The events specified in the "Auditable Event" column of Table 14].**

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, **[the information specified in the "Additional Collected Information" column of Table 14].**

Table 14: Auditable Event

Auditable Event	*Additional Collected Information*
All use of the identification and authentication mechanisms	**The user identity if provided**
All operations performed on users and user rights, for example, adding, deleting, and modifying user information changing passwords, and modifying user rights	**User identity**
All operations performed on authentication types and password policies	**User identity**
All operations performed on virtual resources, including allocating, starting, and stopping a VM	**User identity and VM ID**
All operations performed on resource scheduling policies	**User identity**

6.2.1.2 FAU_GEN.2 User identity association

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.

6.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[administrator or authorized user]** with the capability to read **[audit events listed in Table 14]** 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.

Dependencies: **FAU_GEN.1 Audit data generation**

6.2.1.3 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.4 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[querying]** of audit data based on **[operation, component, level, operation result, operator, IP address, operation time, detail information, failure cause].**

6.2.1.5 FAU_STG.1 Protected audit trail storage

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.

6.2.1.6 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **[delete oldest audit records every hour]** if the audit trail exceeds **[100,000 entries].**

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[FusionManager access control policy]** on

[Subject: users

Objects: objects in domain，objects in organization

Operation: All operations to objects in domain or organization, such as add host, add storage, query logs, query alarms, Create VM, VM power on, VM power off, VM resume, VM migrate etc]

6.2.2.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **[FusionManager access control policy]** to objects based on the following:**[**

a) users and their following security attributes:

i. **username**

ii. **user type (system manager or service manager)**

iii. **resource domain (system manager) or organization (service manager)**

iv. **role**

b) objects and their following security attributes：

domain name，organization name

c) Operation and their following security attributes：operation name].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[Only authorized user whose user name is in granted user list of resource domains or organizations is granted access]**

FDP_ACF.1.3 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: **[none]**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[none]**

6.2.2.3 FDP_IFC.1(1) Subset information flow control- VM Data

FDP_IFC.1.1 The TSF shall enforce **[VM domain isolation policy]** on

[Subjects: Virtual Machine

Information: VM Data in memory and virtual disk

and all operations that cause VM memeory scale up or

down，and read/write virtual disk]

6.2.2.4 FDP_IFF.1(1) Simple security attributes- VM Data

FDP_IFF.1.1(1) The TSF shall enforce the **[VM data isolation policy]** based on the following types of subject and information security attributes**[**

Subject: Virtual Machine

Subject security attributes: virtual addresses, physical addresses, machine addresses, virtual disk ID, instruction queue

Information: VM memory data, VM disk IO，instruction

Information security attributes: None].

FDP_IFF.1.2(1) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **[**

The VM uses the Memory Virtualization technology to virtualize the physical memory and isolate the virtual memory. Based on the mapping mechanism between virtual addresses and the machine addresses of clients, the OS on a VM translates the virtual address into the physical address. The hypervisor then translates the physical address of a client into a machine address, and sends the machine address to the physical server. The hypervisor manages memory mapping and keeps virtual memory isolated.

All disk I/O operations on a VM are intercepted and processed by back-end driver in Dom0, so that the VM can access only the physical disk space allocated to it. The hypervisor controls communication between the front-end driver in the domU guest OS and the back-end driver in the domain 0 and distribute I/O messages by virtual disk ID.

The Hypervisor prevents the Guest OS of VMs from executing all the privileged instructions and isolates the OS from applications.The Hypervisor maintains instruction queue for every vCPU and schedules instructions to be executed.**]**

FDP_IFF.1.3(1) The TSF shall enforce [**none**].

FDP_IFF.1.4(1) The TSF shall explicitly authorise an information flow based on on the following rules: [**none**]

FDP_IFF.1.5(1) The TSF shall explicitly deny an information flow based on on the following rules: [**none**]

6.2.2.5 FDP_IFC.1(2) Subset information flow control- VM Network

FDP_IFC.1.1 The TSF shall enforce **[vSwitch Information flow control SFP]** on

[Subjects:VM virtual network interfaces and physical network interfaces

Information: network data packets

Operations: all operations that cause that information to flow to and from subjects covered by the SFP].

6.2.2.6 FDP_IFF.1(2) Simple security attributes- VM Network

FDP_IFF.1.1(2) The TSF shall enforce the **[vSwitch Information flow control SFP]** based on the following types of subject and information security attributes**[**

Subject: VM virtual network interfaces and physical network interfaces

Subject security attributes: interface ID, MAC,VLAN ID

Information: network data packets

Information security attributes: source and destination interface ID].

FDP_IFF.1.2(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 data packet originates from a recognized physical network interface or VM virtual network interface as identified by the interface identifier or VLAN ID (if applicable), and is addressed to a recognized destination interface which found out by MAC and VLAN ID, then allow the information flow, otherwise deny the information flow].

FDP_IFF.1.3(2) The TSF shall enforce [**none**].

FDP_IFF.1.4(2) The TSF shall explicitly authorise an information flow based on on the following rules: [**none**]

FDP_IFF.1.5(2) The TSF shall explicitly deny an information flow based on on the following rules: [**none**]

6.2.2.7 FDP_RIP.1 Subset residual information protection

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***deallocation of the resource from***] the following objects: [**memory mapped to a virtual machine**].

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[default: 5, configurable]** unsuccessful authentication attempts occur related to **[user logging in].**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***[met]*****,** the TSF shall **[lock user until unlock by system manager or automatic unlock after 10 minutes, configurable].**

6.2.3.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

[

a) username

b) password

c) authentication type

d) resource domain or organization

e) role

f) start time and end time that allow login

g) lock status]

6.2.3.3 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[**

a) at least one lower-case alphanumerical character

b) at least one upper-case alphanumerical character

c) at least one numerical character

d) an administrator configurable combination of the following:

i. contain special character

ii. reject contain username or reversed username

e) an administrator configurable minimum and maximum password length (default minimum length is 6 and maximum is 32 characters)].

6.2.3.3 FIA_UAU.2 User authentication before any action

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

6.2.3.5 FIA_UID.2 User identification before any action

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 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behavior

FMT_MOF.1.1 The TSF shall restrict the ability to ***[determine the behavior of]*** all the functions **[defined in FMT_SMF.1]** to **[administrators or administrator-defined roles]**.

6.2.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[FusionManager access control policy]** to restrict the ability to ***[query, modify]*** the security attributes **[identified in FDP_ACF.1 and FIA_ATD.1]** to the **[administrators or administrator-defined roles]**.

6.2.4.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[FusionManager 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 **[administrators or administrator-defined roles]** to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[**

- **a) configuration of password policy**
- **b) configuration of authentication failure handling policy**
- **c) user management (creation, deletion, modification of lockout status or password)**
- **d) definition of resource domain and organization**
- **e) definition of IP addresses and address ranges that will be accepted as source addresses in client session establishment requests**
- **f) idle user session timeout duration**
- **g) configuration VLAN for VM**
- **h) configuration vcpu，memory，disk quotas for VM]**

6.2.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles **[**

- **a) System management role**
  - **1) administrator**
  - **2) operator**
  - **3) auditor**
- **b) Service management role**

1) **vdcmanager**
2) **user**

c) **other administrator-defined roles].**

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

6.2.5 TOE access (FTA)

6.2.6.1 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after **[default 10 minutes, a time interval of user inactivity which can be configured].**

6.2.6.2 FTA_TSE.1 TOE session establishment

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **[**

a) **valid username and password**
b) **source IP address**
c) **login start and end time**
d) **user lock status**
e) **password expiration date]**

6.2.6 Trusted Path/Channels (FTP)

6.2.6.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **[*remote,OSS*]** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **[*modification, disclosure*].**

FTP_TRP.1.2 The TSF shall permit **[*remote users,OSS user*]** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **[*initial user authentication,* remote management]**.

6.2.7 Protection of the TSF(FPT)

6.2.7.1 FPT_ITT.1 Internal TOE TSF data transfer protection

FPT_ITT.1.1 The TSF shall protect TSF data from ***[disclosure, modification]*** when it is transmitted between separate parts of the TOE.

6.3 Security Functional Requirements Rationale

6.3.1 Security Requirements Dependency Rationale

Dependencies within the EAL3 package selected for the security assurance requirements have been considered by the authors of CC Part 3 and are not analyzed here again.

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirements. The security assurance requirements in this Security Target also do not introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Table 15: Dependencies between TOE security functional requirements

Security Functional Requirement	Dependency	Resolution
FAU_GEN.1	FPT_STM.1	OE
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1

FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FDP_IFC.1(1)	FDP_IFF.1	FDP_IFF.1
FDP_IFC.1(2)	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1(1)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FDP_IFF.1(2)	FDP_IFC.1 FMT_MSA.3	FDP_IFC.1 FMT_MSA.3
FDP_RIP.1	No Dependencies	None
FPT_ITT.1	No Dependencies	None
FIA_AFL.1	FIA_UAU.2	FIA_UAU.2
FIA_ATD.1	No Dependencies	None
FIA_SOS.1	No Dependencies	None
FIA_UAU.2	FIA_UID.2	FIA_UID.2
FIA_UID.2	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FDP_IFC.1(1) FDP_IFC.1(2) FMT_SMR.1 FMT_SMF.1

FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.1
FTA_SSL.3	No Dependencies	None
FTA_TSE.1	No Dependencies	None
FTP_TRP.1	No Dependencies	None

6.3.2 Sufficiency and Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Table 16: Mapping SFRs to objectives

	O.Authentication	O. Authorization	O. Communication	O.Audit	O.VM_DOM_ISO	O.VNETWORK_ISO
FAU_GEN.1				X		
FAU_GEN.2				X		
FAU_SAR.1				X		
FAU_SAR.2				X		
FAU_SAR.3				X		
FAU_STG.1				X		
FAU_STG.3				X		
FDP_ACC.1		X				

FDP_ACF.1		X				
FDP_IFC.1(1)					X	
FDP_IFC.1(2)						X
FDP_IFF.1(1)					X	
FDP_IFF.1(2)						X
FDP_RIP.1					X	
FPT_ITT.1			X			
FIA_AFL.1	X					
FIA_ATD.1		X				
FIA_SOS.1	X		X			X
FIA_UAU.2	X					X
FIA_UID.2	X					
FMT_MOF.1		X				
FMT_MSA.1		X				
FMT_MSA.3		X				
FMT_SMF.1		X		X		
FMT_SMR.1		X				
FTA_SSL.3	X					
FTA_TSE.1	X					
FTP_TRP.1			X			

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable.

Table 17: SFR sufficiency analysis

Objective	SFRs	Rationale
O.VM_DOM_ISO	FDP_IFC.1(1) FDP_IFF.1(1) FDP_RIP.1	These SFRs apply UVP to keep domain isolation.
O.VNETWORK_ISO	FDP_IFC.1(2) FDP_IFF.1(2)	These SFRs apply vSwitch/VLAN/ACL based port to limit network packets going to the VM and thereby ensure that only protected traffic goes through.
O.Communication	FTP_TRP.1 FPT_ITT.1 FIA_SOS.1	This SFR provides the secure communication between users and management interface of the TOE. Offer trusted path for O&M.
O.Authentication	FIA_UID.2 FIA_UAU.2	These SFRs ensure that a user must identify and authenticate by password.
	FTA_TSE.1 FIA_AFL.1 FTA_SSL.3 FIA_SOS.1	The SFRs support authentication by: • Refusing logins from certain IP addresses • Not allowing unlimited login attempts • Logging out users after an inactivity period • Ensuring password quality
O.Authorization	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized administrators can access certain functions
	FMT_SMR.1	These SFRs define authorization role and

	FIA_ATD.1	ensure that upon login an administrator gets the proper authorization role.
	FMT_MOF.1 FMT_SMF.1	These SFR lists certain management functions and restricts them to the proper authorization role.
	FMT_MSA.1 FMT_MSA.3	These SFRs ensure that new system administrator or service administrator only get limited access rights and specifies who can modify these access rights.
O.Audit	FAU_GEN.1 FAU_GEN.2	These SFRs ensure that audit records can be generated of significant events and that these contain useful information, including the correct time of the events.
	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3	These SFRs ensure that the correct users can read the correct information from the audit records.
	FAU_STG.1 FAU_STG.3	These SFRs ensure the audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

6.5 Security Assurance Requirements Rationale

The evaluation assurance level 3 augmented with ALC_FLR.2, has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functional Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

7.1.1 Security Audit

An operation log records the operation a user has performed on the system and the result of the operation and is used for tracing and auditing.

Fields contained in an operation log include:

- Operation name (type)
- Component name
- Operator
- IP address used by the operator
- Log level
- Operation time
- Operation result
- Detailed operation information
- Failure cause

Only administrators who are granted log query rights can query and export operation logs. Logs cannot be modified or deleted on the management portals.

The TOE allows users to query operation logs by specifying search criteria. The search criteria can be any field contained in an operation log. The operation logs of the TOE can be exported to a local directory for auditing.

The FusionManager checks the number of operation logs every hour. If the number of logs exceeds 100, 000, the TOE automatically deletes the earliest logs.

The Security Audit function is designed to satisfy the following security functional

requirements:FAU_GEN.1,FAU_GEN.2,FAU_SAR.1,FAU_SAR.2,FAU_SAR.3,FAU_STG.1,FAU_STG.3

7.1.2 System Management

The TOE automatically terminates the session for the communication between the management portal and the background management program if users do not perform any operation on the portal within a specified time period (10 minutes by default and configurable).

The TOE supports an external NTP clock source. If no external clock source is configured, the TOE uses the time of the OS.

The System Management function is designed to satisfy the following security functional requirements:FTA_SSL.3

7.1.3 User and Privilege Management

The access control policies that control access from VM users to VMs through user network plane are managed by VMs. The TOE does not manage these policies. Therefore, this section only describes the access control function provided by the TOE for system maintenance personnel to access the virtualization platform and VMs.

The TOE supports role-based access control. Administrators are assigned different rights in different domains and organizations to control the rights of the administrators. By managing users, roles, domains, and organizations, operations performed by different users in different organizations are independent from one another, which achieves data isolation.

- User management

  Administrators can create, modify, and delete users in the system.

  System administrators can create users with the rights to manage the system. When creating a user, the system administrator must specify the resource domains that can be managed by the user.

  When creating an organization, a system administrator must create a service administrator that manages the organization.

  Service administrators can create users with the rights to manage services in the organization.

- Role management

Administrators can define different combinations of rights by role and grant specific rights to different roles.

The TOE provides the following two roles:

- Role type
  - System administrator: has rights to manage the system, resources, and faults.
  - Service administrator: has rights to manage catalogs, application instance, and organization resources.
- Default roles

The TOE provides the following default roles:

- System administrator: system super administrator, system operator and auditor
- Service administrator: VDC administrator and VDC user

➢ Domain management

- Domain-based resource management

System administrators can create different domains and associate resource clusters with the domains to implement domain-based resource management.

- Domain-based user management

System administrators can grant users different rights based on the domain to which the users belong. Domains are defined for system administrators. A system administrator can manage multiple domains, and a domain can be managed by multiple system administrators.

- Rights- and domain-based management

System administrators have different rights in different domains by implementing rights- and domain-based management. Users in different resource clusters also have different rights.

➢ Organization management

- Resources

Organizations are associated with virtual resources. System administrators can create organizations and allocate VDCs to specific organizations.

- Users

Organizations are associated with users. After system administrators allocate a VDC to an organization, organization administrators in the organization can manage the VDC based on their roles. Organizations are defined for service administrators. A service administrator can manage multiple organizations, but an organization can only be managed by a service administrator.

- VDCs

It is the logical allocation of computing, storage, and network resources in the resource clusters by user or cluster. The VDC contains only virtual resources.

- FusionManager access control policy management
  - A system administrator can perform specified operations on resources in a domain only after the system administrator is granted domain- and operation-related rights.
  - Service administrators are associated with organizations and can only perform specified operations on resources in the associated organization.
  - Only system administrators and other authorized users can access security management modules.

The User and Privilege Management function is designed to satisfy the following security functional requirements:FDP_ACC.1,FDP_ACF.1,FIA_ATD.1,FMT_MSA.1,FMT_MSA.3,FMT_SMF.1,FMT_SMR.1, FMT_MOF.1

7.1.4 Authentication and Authorization

When a user logs into the FusionSphere system, a username and password are requested to verify the user before the access is given. FusionSphere will also verify,

- If the client IP address is in the specific client IP addresses that can be used to remotely access the management interface
- If the login time is in the permitted login start time and end time.
- If the password is overdue

The user can log in to the FusionSphere system and obtain related rights only after the user is authenticated.

The TOE supports the local username and password authentication. Usernames used in the local username and password authentication are stored in the data table, and the passwords are encrypted using SHA256.

Administrators can configure password policy and specific client IP addresses who can remotely access the management interface.Password must meet the following base requirements:

- The password is a string of 8 to 32 characters.
- The password must contain at least two of the following combinations:
    1. Lowercase letters
    2. Uppercase letters
    3. Digits
- The password must comply with the pre-configured password policies:
    - Minimum length
    - Maximum length
    - Contain special characters
    - Allow username or reversed username
    - Rules on using the same password
    - Password validity (days)
    - Forcibly change password upon initial login
    - Minimum change interval (minutes)
    - Advance warning of password expiry (days)
    - Maximum number of incorrect passwords allowed
    - Statistics period (minute)
    - User locking duration (minutes)

If a user fails to be authenticated for several consecutive times (5 by default and configurable) within a specified time period (5 minutes by default and configurable), the TOE automatically locks the user within a specified time period (10 minutes by default and configurable).After a user successfully logs in to the system and performs an operation on the system, the TOE authenticates the operation based on the user

ID, domain or organization to which the user belongs, and operation ID. If the authentication fails, the TOE forbids the operation.

Both failed and successful login events are recorded in the login logs.

The Authentication and Authorization function is designed to satisfy the following security functional requirements:FIA_UID.2,FIA_UAU.2,FIA_AFL.1,FIA_SSL.3，FIA_SOS.1，FTA_TSE.1

7.1.5 Communication protection

Data transmitted between FusionManager and FusionCompute can be encrypted using Transport Layer Security (TLS)/SSLv3.

Data transmission between the front-end and back-end can be encrypted using TLS/SSLv3 when a user accesses the FusionManager portal.

Data transmission through the FusionManager northbound interfaces can be encrypted using TLS/SSL when the 3rd-party OSS accesses the FusionManager northbound interfaces.

The Cryptographic Support function is designed to satisfy the following security functional requirements: FPT_ITT.1,FTP_TRP.1

7.1.6 VM Domain Separation

- Separation between physical resources and virtual resources

Each virtual machine is isolated from other virtual machines running on the same hardware. Although virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system on an individual virtual machine cannot detect any device other than the virtual devices made available to it. All physical hardware accesses are mediated by Hypervisor to guarantee one VM only can access the physical resources which are assigned to it. Furthermore, if one VM is broken down, it does not compromise the hypervisor or other VMs.

- CPU Scheduling Isolation

Huawei FusionSphere uses x86 architecture servers. The x86 architecture offers 4 privilege levels ranging from ring 0 which is the most privileged, to ring 3 which is the least privileged. OS core runs in ring 0. OS services run in ring 2, and user applications run in ring 3. The Hypervisor prevents the Guest OS of VMs from executing all the privileged instructions and isolates the OS from applications.The

Hypervisor maintains instruction queue for every vCPU and schedules instructions to be executed.

- Memory Separation

The TOE uses the memory virtualization technology to implement memory isolation among VMs. The memory virtualization technology introduces the physical address based on the existing mapping between virtual addresses and the machine addresses of VMs. The VM OS translates the virtual address into the physical address. The hypervisor first translates the physical address of the VM into a machine address, and then sends the machine address to the physical server.

In memory-sharing scenario, when the recycled memory space put into reuse , the physical bits of memory will be writen ‘0’ to ensure data security.

The VM Domain Separation function is designed to satisfy the following security functional requirements: FDP_IFC.1(1),FDP_IFF.1(1),FDP_RIP.1

7.1.7 VM Storage Separation

The TOE uses the front-end and back-end drivers to enable the communication between VMs and VM disks. Front-end drivers must be installed on VMs and work together with the back-end driver in Domain 0 to enable the VMs to effectively access their disks using the mechanisms provided by the Virtual Machine Manager (VMM). The front-end and back-end drivers allow the TOE to provide better disk I/O performance. Different VMs have different front-end drivers, which helps to achieve VM disk I/O isolation

If a virtual disk is allocated to a VM, the disk cannot be allocated to another VM.

The VM Storage Separation function is designed to satisfy the following security functional requirements:FDP_IFC.1(1),FDP_IFF.1(1)

7.1.8 VM Network Separation

The TOE supports virtual switches and VLANs. Administrators or authorized users can configure network isolation policies on the management portal.

A virtual switch has all the functions provided by a physical switch. The virtual switch functions are implemented only by software. The TOE provides the VPN Routing and Forwarding (VRF) function. Each VM has one or multiple Virtual Interfaces (VIFs) that

logically belong to the VRF. Data transmission between two VMs is implemented as follows:

- A data packet sent from the source VM first reaches the back-end driver of Domain 0.
- The back-end driver sends the packet to the virtual switch.
- The virtual switch parses the layer 2 message header, extracts the source and destination identifiers, filters the data, performs an integrity check, and sends the data packet to the target VIF.
- The back-end driver sends the packet to destination VM.
- The destination VM checks the data packet and determines whether to accept it.

vSwitch supports such layer 2 network security policies as for preventing IP or MAC address spoofing.IP-MAC address binding prevents IP address or MAC address spoofing initiated by changing the IP address or MAC address of a VM NIC, and therefore enhances network security of user VMs. With this policy enabled, an IP address is bound to an MAC address using the DHCP snooping technique, and then the packets from untrusted sources are filtered using IP Source Guard and dynamic ARP inspection (DAI).

The VM Network Separation function is designed to satisfy the following security functional requirements:FDP_IFC.1(2),FDP_IFF.1(2)

8 Abbreviations, Terminology and References

8.1 Abbreviations

ACL	Access Control List
AD	Activity Directory
CC	Common Criteria
CNA	Compute Node Agent
FTP	File Transfer Protocol
GUI	Graphical User Interface
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure

NTP	Network Time Protocol
O&M	Operation and Management
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions
UVP	Universal Virtualization Platform
VDC	Virtual Data Center
VLAN	Virtual Local Area Network
VM	Virtual Machine
VRM	Virtualiztion Resoures Management
VRF	Virtual Router Function
VIF	Virtual Interface
OSS	Operating Support System

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

user: A user is a adminstrator of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE's point of view, an administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.

VM User:	A user is a human or a product/application using VM.
Management VM	Virtual machine used to deploy management components, such as FusionManager，VRM etc.
user VM:	VM is for end user, vs managemenet VM.
Domain 0:	*A special-purpose domain (based on a Linux kernel) that exists in a single instance on each host. Domain 0 is the only privileged domain on a host, and is thus the only domain that can control access to physical input/output resources directly and access the content of other domains (Domain U).*
Domain U	*The collection of domains other than Domain 0. Each of these domains is a VM, on which a guest operating system has been (or will be) installed.*
Hypervisor	An abstraction layer implementing a set of software calls that can be made by domains, and providing an asynchronous event-based interface for communication from the hypervisor to domains. The hypervisor controls the scheduling of the CPU and the partitioning of memory between virtual machines.

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation. September 2012. Version 3.1 Revision 4.