Platform Computing Inc.
3760 14th Avenue
Markham, Ontario L3R 3T7
Canada

Tel: (905) 948-8448
Fax: (905) 948-9975

email: info@platform.com
www.platform.com

PLATFORM
LSF HPC 6.2
Security Target EAL 2

Prepared for:

Platform Computing Inc.
3760 14th Avenue
Markham, ON
L3R 3T7

Prepared by:

AEPOS Technologies Corporation
200 Montcalm Street, Suite 200
Gatineau, Quebec
J8Y 3B5

Client Contract No.: CS1557.008
Date: February 21, 2006

Platform™

DOCUMENT ORIGIN AND APPROVAL RECORD

Prepared by: _____ _____

D. White
IT Security Consultant

Date

Prepared by: _____ _____

N. MacAskill
Senior IT Security Consultant

Date

Reviewed by: _____ _____

G. Jenson, P.Eng, PMP
Manager, IT Security Engineering

Date

Approved by: _____ _____

J. Detombe
Director, IT Security

Date

Accepted by: _____ _____

I. Mackay
Director, Engineering Operations

Date

Platform™

REVISION HISTORY

Date of Issue	Revision Number	Description of Change
November 14, 2005	.01	Initial Release
November 25, 2005	.02	Incorporated comments provided to AEPOS from Platform (comments received on November 22)
December 15, 2005	.03	Incorporated OR comments received from DOMUS
January 4, 2006	.04	Removed reference to version 6.2x and replaced with 6.2
January 6, 2006	.05	Incorporated OR comments received from CSE
January 11, 2006	.06	Changed Assurance Documentation names
February 14, 2006	.07	Removed the word "query" from FMT_MTD.1.1 Added additional resource "CPU time limit" to FRU_RSA.1.1
February 15, 2006	.08	Changed the name of AM_ATE_FUN document. Additional minor changes required for the document to be consistent with changes in revision .07
February 21, 2006	.09	Clarified ITSF_ADMIN section on pages 23 and 24

Platform™

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ANNEXES

Platform Computing Inc.
3760 14th Avenue
Markham, Ontario L3R 3T7
Canada

Tel: (905) 948-8448
Fax: (905) 948-9975

email: info@platform.com
www.platform.com

1. INTRODUCTION TO THE SECURITY TARGET

1.1 Security Target Identification

Title:	Platform Load Sharing Facility (LSF) High Performance Computing (HPC) 6.2 Security Target EAL 2
Product:	Platform LSF HPC 6.2
ST Revision Number:	.06 DRAFT
Manufacturer:	Platform Computing Inc.

1.2 Security Target Overview

This ST describes the IT security requirements for the Platform's LSF HPC 6.2 software. The LSF HPC 6.2 software manages batch compute jobs on clusters of computer systems. Users use the LSF to submit jobs that require significant CPU time, memory, and/or disk space. Several server processes running on each system co-ordinate to distribute the load across the cluster. User jobs are submitted using the LSF HPC 6.2 queuing software and the LSF HPC determines where jobs will be run. The LSF software requires support from the underlying operating system for some security functionality. For the purpose of this evaluation the operating system is Red Hat Enterprise Linux AS version 3 Update 3. This version of Linux has been CC certified at the EAL 3+ level.

The LSF HPC can:

- Utilize computing resources at maximum capacity;
- Take full advantage of high performance network interconnects available on clustered systems and supercomputers;
- Use topology-based scheduling that enables maximum application performance for industry leading interconnects;
- Provide scalability and performance; and
- Utilize an extensive library of third party application integrations.

1.3 CC Conformance Claim

The Target of Evaluation (TOE) is conformant with:

- CC Version 2.2 Part 2; and
- CC Version 2.2 Part 3

1.4 Protection Profile Conformance Claim

This ST does not claim conformance to any Protection Profile.

1.5 Security Target Organization

The main sections of the ST are the target of evaluation (TOE) description, TOE security environment, security objectives, IT security requirements, TOE summary specification, rationale, and annexes.

The TOE description provides general information about the TOE, defines the evaluated configuration for the TOE, and serves as an aid to understanding its security requirements.

The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. The TOE security environment includes:

- assumptions regarding the TOE's intended usage and environment of use;
- threats relevant to secure TOE operation; and
- organizational security policies with which the TOE must comply.

The security objectives reflect the stated intent of the TOE and its environment. They pertain to how the TOE will counter identified threats and how it will cover identified organizational security policies and assumptions. Each security objective is categorized as being for the TOE or for the environment.

The security requirements section provides the IT security requirements as follows:

- TOE security functional requirements (SFRs);
- TOE security assurance requirements (SARs); and
- IT environment security functional requirements.

The TOE summary specification (TSS) provides a description of the TOE security functions (TSF) that the TOE provides in order to satisfy the SFRs. The TSS also describes the assurance measures that will be used to satisfy the SARs. The determination of whether or not the TSFs and SARs satisfy the security requirements is the objective of the TOE evaluation.

The rationale presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The rationale is in three main parts. First, a security objectives rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a security requirements rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them. Finally, a TOE summary specification rationale demonstrates that the TOE security functions and assurance measures are traceable to the security requirements and are suitable to meet them.

1.6 Related Standards and Documents

1. Common Criteria Version 2.2 - Common Criteria for Information Technology Security Evaluation; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements.

2. Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 2.2.

2. TARGET OF EVALUATION DESCRIPTION

The Target of Evaluation (TOE) is the LSF HPC 6.2. The TOE logical boundary is considered to be the LSF HPC 6.2 software. The TOE is installed and operated on one or more hosts. Hosts are defined as an individual computer in the cluster. The group of hosts running the software work together as a single unit, combining computing power and sharing workload and resources. The TOE includes the Multi-Cluster option which allows for organizations to have separate, independently managed clusters. Communication between the clusters is secured using Stunnel, which is an SSL encryption wrapper that wraps around standard, non-secure network traffic for certain services and prevents interceptors from being able to "sniff" the communication between client and server[1].

The TOE requires support from the underlying operating system for some security functionality. For the purpose of this evaluation the operating system is Red Hat Enterprise Linux AS version 3 Update 3. This version of Linux has been CC certified at the EAL 3+ level.

2.1 TOE Functional Description

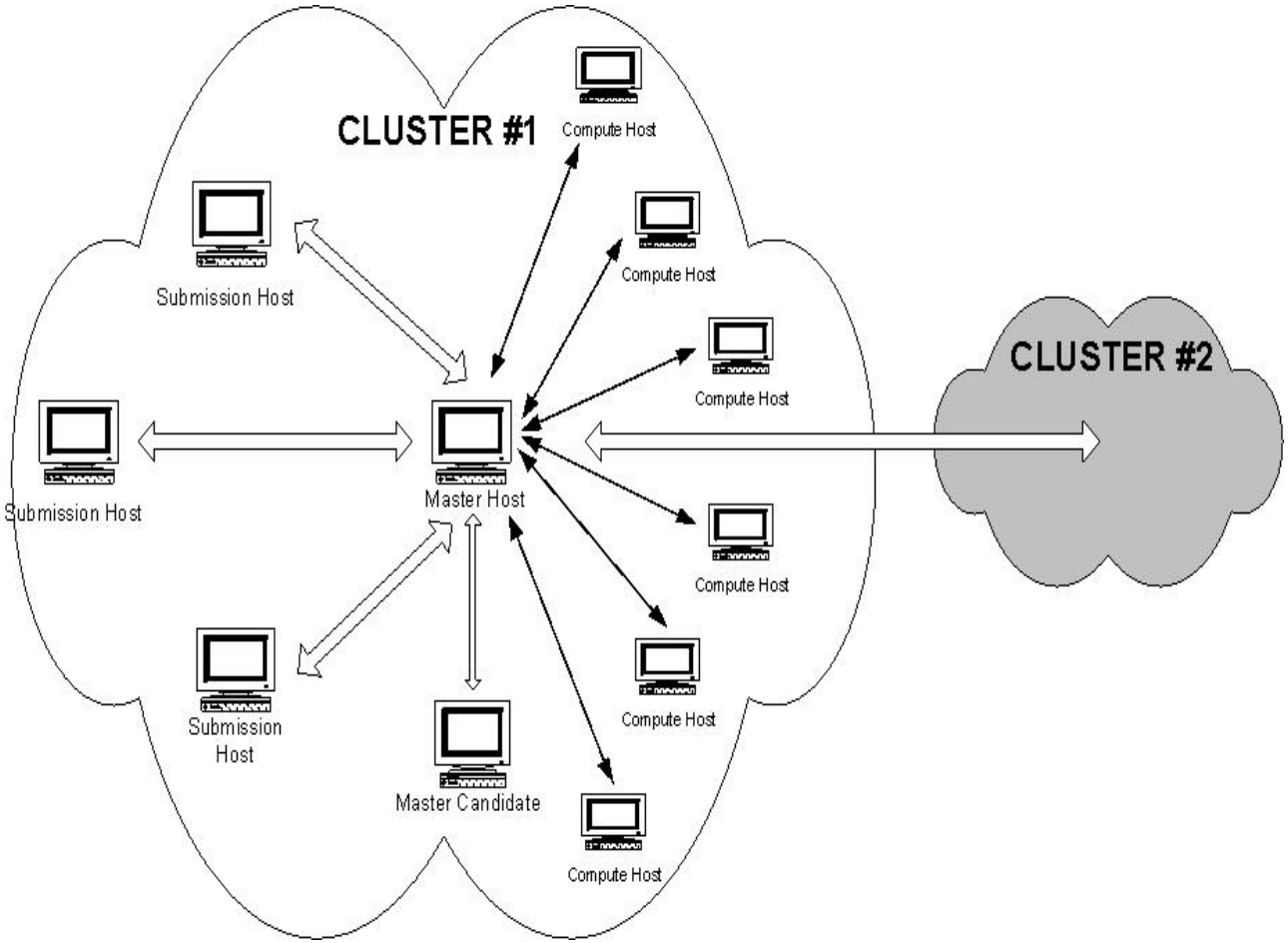
Diagram 2.1 is a general representation of the LSF environment. The Platform LSF HPC provides a multiprocessing computing environment that permits software applications (jobs) to run concurrently on several different hosts (processors), thus reducing the execution time. The Platform LSF HPC is comprised of one or more clusters, each of which includes the following:

- Submission Hosts which are responsible for submitting jobs that require processing.
- A Master Host which controls the allocation of these jobs to the hosts that will perform the processing. The Master acts as a coordinator for the Cluster, performing all the scheduling and dispatching tasks.
- Compute Hosts, also called Execution Hosts, which are responsible for executing the jobs that have assigned to them.
- A Master Candidate Host which is a Server (Compute or Submission) which can assume the role of Master Host in the event of a failure on that system.

[1] Stunnel is a security function provided by the IT environment.

All hosts take on the designations of Client or Server. A Client, as typified by a Submission Host, is only capable of submitting jobs to the Master. It cannot assume any other role. A Server is capable of submitting jobs, like a Client, but it is also capable of performing the Master Host and computing functions (Compute Host). In the event that the Master Host goes down, one of the Server Hosts called a Master Candidate will assume its role.

Figure 2.1 – Platform LSF HPC Computing Environment



Before being processed by the Master Host, all batch jobs are placed in a queue. Queues are system-wide, i.e., they are not associated with a specific host. It is the job of the Master Host to determine which Compute Host is to receive the job. Each queue is defined by a unique set of job control and execution parameters. It is also possible to submit interactive jobs to a queue. In this case, I/O is directed to a session running on a specific terminal where the job originated. The interactive session must be completed before the next job can be submitted to that session.

The following daemons, which run on the various LSF HPC hosts, make up the logical boundary of the TOE:

- **Master Batch Daemon (mbatchd)** – This daemon provides job request and dispatch functionality and runs on the master host. This daemon is responsible for the overall state of jobs in the system. It receives job submission, and information query requests, manages jobs held in queues and dispatches jobs to hosts as determined by mbschd.

- **Master Batch Scheduler Daemon (mbschd) –** This daemon makes scheduling decisions based on job requirements and policies. This daemon runs on the master host.

- **Slave Batch Daemon (sbatchd)** - The Slave Batch Daemon runs on each server host. This daemon receives the request to run the job from mbatchd and manages local execution of the job. It is responsible for enforcing local policies and maintaining the state of jobs on the host. sbatchd forks a child process for every job. The child sbatchd runs an instance of res to create the execution environment in which the job runs. The child sbatchd exits when the job is complete.

- **Remote Execution Server (RES)** – RES runs on each server host. It accepts remote execution requests to provide transparent and secure remote execution of jobs and tasks.

- **Load Information Manager (LIM)** – The LIM runs on each server host. The LIM collects host load and configuration information and forwards it to the master LIM running on the master host.

- **Master LIM** - The Master LIM runs on the master host. It receives load information from the LIMs running on hosts in the cluster. It forwards load information to mbatchd, which forwards this information to mbschd to support scheduling decisions. If the master LIM becomes unavailable, a LIM on another host automatically takes over.

- **Process Information Manager (PIM)** - PIM runs on each server host. It is started by LIM, which periodically checks on pim and restarts it if it dies. It collects information about job processes running on the host such as CPU and memory used by the job, and reports the information to sbatchd.

A mapping of daemons to hosts is shown in Table 2.1.

Table 2.1- Daemon Allocation

	Master	Submission	Execution
Daemon			
mbatchd	X		
mbsched	X		
sbatchd	X	X	X
RES	X	X	X
Master LIM	X		
LIM		X	X
PIM	X	X	X

2.2 Features

The primary security features offered by the TOE with support from the IT environment are as follows.

2.2.1 Access Control

Role based access control is enforced for the Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue user and Any User roles. An access request is granted or denied based on a set of configuration files that define user-to-role and role-to-authorization mappings.

2.2.2 Audit

The TOE provides an audit capability that generates audit records for security critical events.

2.2.3 Identification and Authentication

The TOE with support from the Linux OS provides user identification and authentication functionality. Authentication is the process of identification of a user, device or other entity, (typically based on a password or pass phrase) known only to a single user, which when paired with the user's identification allows access to a secure resource. The TOE validates user accounts at the system level, which enables the user account to be to be valid on all hosts. Users must have valid accounts on all hosts. This allows any user to run a job with their own permissions on any host in the cluster.

2.2.4 Security Management

The TOE provides roles to manage security functions. Only authorized roles are permitted to manage the TOE and perform administrative functions.

2.2.5 Protection of TOE Security Functions

The TOE with support from the IT environment provides reliable timestamps via the OS's internal real time clock. The underlying OS ensures that the TOE Security Policy enforcement functions are invoked and succeed before each function within the TOE Scope of Control (TSC) is allowed to proceed. The underlying OS maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

2.2.6 Resource Allocation

The TOE provides the functionality to allocate resource limitations to ensure that a user or process cannot monopolize a resource and cause a denial of service.

2.2.7 User and Authentication Data Protection

The TOE with support from the environment provides both user and authentication data protection. User and authentication data, which is communication between the clusters, is secured using Stunnel. Stunnel is an SSL encryption wrapper that wraps around standard, non-secure network traffic for certain services and prevents interceptors from being able to "sniff" the communication between client and server.

3. TOE SECURITY ENVIRONMENT

This section identifies the security problem that exists with the protection of identified assets. The security problem is expressed as threats and policy that the TOE, operating in its environment, must address. For the TOE to fulfill its security requirements, specific conditions must be upheld in the operating environment. These conditions are expressed as assumptions.

3.1 Assets

The assets of concern to this ST are defined as follows:

- **LSF Users**. LSF users are defined as a user account which has permission to submit jobs to the LSF cluster.
- **Administrative Users.** Administrative users are defined as those users required to configure and manage the TOE.

- **Information.** User data held within the LSF including data in transit between remote hosts.

- **TSF data.** TSF data is defined as data that is required to support the secure operations on the data held within the LSF. This data includes: authentication data, configuration data/files, audit data, access control attributes such as permission bits.

- **Objects.** Objects are defined as cluster, queue, job and host. The TOE's role based access control policy governs subject access to the identified objects.

3.2 Statement of Assumptions

The specific conditions listed below are assumed to exist in the LSF HPC operating environment. Each assumption is stated in bold type font. An application note, in normal font, which supplies additional information and interpretation, follows it.

3.2.1 Personnel Assumptions

A.TRUSTED_ADMIN
The system administrative personnel are trusted and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator/user documentation. Furthermore, the administrators of the TOE have been adequately trained in order for them to securely configure the TOE.

3.2.2 Physical Assumptions

A.PHYSICAL
The TOE resides in a controlled and physically secure environment.

3.3 Statement of Threats

The following threats are addressed by the TOE operating in its intended environment or by technical security measures provided by the IT environment or by non-technical security measures (personnel, procedural and physical measures) in the environment.

3.3.1 Threats Countered by the TOE

T.DENIAL_OF _SERVICE
A TOE user or process could monopolize TOE resources thereby causing denial of service.

T.ACCESS
A TOE user could gain access to objects they are not permitted access to.

3.3.2 Threats Countered by the IT Environment

T.E.TRANSIT
Data transferred between nodes is disclosed to or is modified by an authorized user or process.

T.E.ACCESS_TOE
An unauthorized user gains access to the underlying OS, thereby gaining unauthorized access to the TOE.

3.4 Organizational Security Policy

Each policy is stated in bold type font, and is followed by an application note, in normal font, which supplies additional information and interpretation.

P.AUTHORIZED_USERS
Only those users who have been authorized to access the information within the system may access the system.

P.NEED_TO_KNOW
The system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a "need to know" for that information.

P.ACCOUNTABILITY
The users of the system shall be held accountable for their actions within the system.

4. SECURITY OBJECTIVES

4.1 TOE Security Objectives

This section defines the security objectives of the TOE. Security objectives are categorized as either IT security objectives or non-IT security objectives and serve to reflect the stated intent to counter identified threats and/or comply with any organizational security policies identified. Each objective is stated in bold type font. If required, an application note, in normal font, which supplies additional information and interpretation, follows it.

4.1.1 TOE IT Security Objectives

O.ACCESS _CONTROL
The TOE must provide the means to enforce an access control policy among subjects and objects.

O.AUDITING
The TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.

O.ADMIN
The TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

O.AVAILABILITY
The TOE must provide functionality to control the use of resources by users and subjects such that a denial of service will not occur due to the monopolization of TOE resources.

4.2 Environmental Security Objectives

4.2.1 IT Environmental Security Objectives

O.E.I_AND_A
The IT environment must provide the means to identify and authenticate users of the TOE.

O.E.DISCRETIONARY_ACCESS
The IT environment must control access to resources based on the identity of users.

O.E.SECURE _CHANNEL
The IT environment must provide the means to transmit authentication data and user data securely to remote hosts.

O.E.ENFORCEMENT
The underlying OS (IT environment) must be designed and implemented in a manner which ensures that the organizational policies are enforced.

O.E.TIME_STAMPS
The IT environment must provide reliable time-stamps for the audit records.

4.2.2 Non-IT Security Objectives for the Environment

The non-IT Environmental security objectives are as follows.

O.E.PHYSICAL
Those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attack.

O.E.TRUSTED_ADMIN

Those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their management functions.

5. IT SECURITY REQUIREMENTS

This section specifies the Security Functional Requirements (SFRs) for the TOE and the IT environment. All SFRs were drawn from Part 2 of the CC. In the section that follows some SFRs have been iterated as both the TOE and the IT environment perform the security function. To distinguish between the iterations a (1) after the SFR title indicates a security function for the TOE and a (2) after the SFR title indicates a security function for the IT environment.

5.1 Audit

5.1.1 Audit Data Generation (FAU_GEN.1)

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 [selection: *basic*] level of audit; and
c) Auditable events include:

- ***userok: Request from bad port (<port_number>)***
- ***userok: Forged username suspected from <host/<port>***
- ***resControl: Operation permission denied, uid = <uid>***

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, 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 ST:

The audit function will record all write and execute operations on the following:

- ***Configure a cluster;***
- ***Control (start and shutdown) of a cluster;***
- ***Control (open and close) a queue;***
- ***Submit a job;***
- ***Control (suspend, resume, terminate and change a priority of a job);***
- ***Add, configure and delete a host;***
- ***Control (open and close) a host.***

5.1.2 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [assignment: Primary Cluster Administrator] with the capability to read [assignment: all audit 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.

5.1.3 Restricted Audit Review (FAU_SAR.2)

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.

5.2 User Data Protection

5.2.1 Subset Access Control (FDP_ACC.1) (1)

FDP_ACC.1.1 The TSF shall enforce the [assignment: Role Based Access Control Policy] on [assignment: list of subjects, objects and operations among subjects and objects covered by the SFP].

Subjects: ***Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue User, Any User***.
Objects**:** ***Cluster, Queue, Job, Host***
Operations: ***read, write, execute***.

5.2.2 Security Attribute based Access Control (FDP_ACF.1) (1)

FDP_ACF.1.1 The TSF shall enforce the [assignment: Role Based Access Control Policy] to objects based on the following:

a) ***The assigned user role***; and
b) ***The following access control attributes associated with an object: read, write and execute permission bits***.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) ***A subject can access an object only if the subject has been assigned a role***.
b) ***A subject's active role must be authorized for the subject. This rule ensures that users can take on only roles for which they are authorized.***
c) ***A subject can access an object only if the object is authorized for the subject's active role.***

FDP_ACF.1.3 The TSF shall explicitly authorize access of subject to objects based on the following additional rules: [assignment: no additional rules.]

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: subjects can only access objects that are authorized for their role. An attempt to access an object not part of a role will be denied.]

5.3 Security Management

5.3.1 Management of Security Attributes (FMT_MSA.1) (1)

FMT_MSA.1.1 The TSF shall enforce the [assignment: Role Based Access Control Policy] to restrict the ability to [selection: change default, query, modify, delete [assignment: no other operations]] the security attributes [assignment: role assignment, cluster queue and host configuration, resource allocation limits] to [assignment: the Primary Cluster Administrator].

5.3.2 Static Attribute Initialization (FMT_MSA.3) (1)

FMT_MSA.3.1 The TSF shall enforce the [assignment: Role Based Access Control Policy] to provide restrictive default values for security attributes that are used to enforce the Role Based Access Control Policy.

FMT_MSA.3.2 The TSF shall allow the [assignment: the Primary Cluster Administrator] to specify alternative initial values to override the default values when an object or information is created.

5.3.3 Management of TSF Data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: modify, delete] the [assignment: TOE configuration files] to [assignment: the Primary Cluster Administrator].

5.3.4 Specification of Management Functions (FMT_SMF.1) (1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: the audit management function and resource allocation management function, access control function].

5.3.5 Security Roles (FMT_SMR.1) (1)

FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue User, Any User].

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

5.4 Resource Allocation

5.4.1 Maximum Quotas (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: [assignment: job slots by host, job slots by processor, memory, swap space, tmp space, software licenses, CPU time limit] that [selection: defined groups of users] can use [selection: simultaneously and over a specified period of time].

Application Note:
Defined group of users refers to users and user groups, hosts and host groups, queues, all jobs in the cluster.

5.5 SFR Dependencies

Some of the IT Security Functions described above have dependencies. The following table illustrates that the security target has satisfied SFRs which have dependencies and provides remarks for those which are omitted.

Table 5.1: SFR Dependency Table for the TOE

Security Functional Requirement	Dependencies	Remarks
FAU_GEN.1	FPT_STM.1	Included
FAU_SAR.1	FAU_GEN.1	Included
FAU_SAR.2	FAU_SAR.1	Included
FDP_ACC.1 (1)	FDP_ACF.1 (1)	Included
FDP_ACF.1 (1)	FDP_ACC.1 (1), FMT_MSA.3 (1)	Included
FMT_MSA.1 (1)	FDP_ACC.1 (1), FMT_SMF.1 (1), FMT_SMR.1 (1)	Included

Security Functional Requirement	Dependencies	Remarks
FMT_MSA.3 (1)	FMT_MSA.1 (1), FMT_SMR.1 (1)	Included
FMT_MTD.1	FMT_SMR.1 (1), FMT_SMF.1 (1)	Included
FMT_SMF.1 (1)	N/A	N/A
FMT_SMR.1 (1)	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FRU_RSA.1	N/A	N/A

Table 5-2: SFR Dependency Table for the IT Environment

Security Functional Requirement	Dependencies	Remarks
FDP_ACC.1 (2)	FDP_ACF.1 (2)	Included
FDP_ACF.1 (2)	FDP_ACC.1 (2), FMT_MSA.3 (2)	Included
FDP_ITT.1	FDP_ACC.1 (2)	Included
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FIA_UID.2	N/A	N/A
FMT_MSA.1 (2)	FDP_ACC.1 (2), FMT_SMF.1 (2), FMT_SMR.1 (2)	Included
FMT_MSA.3 (2)	FMT_MSA.1 (2), FMT_SMR.1 (2)	Included
FMT_SMF.1 (2)	N/A	N/A

Security Functional Requirement	Dependencies	Remarks
FMT_SMR.1 (2)	FIA_UID.1	Satisfied by FIA_UID.2 which is hierarchical to FIA_UID.1.
FPT_ITT.1	N/A	N/A
FPT_RVM.1	N/A	N/A
FPT_SEP.1	N/A	N/A
FPT_STM.1	N/A	N/A

5.6 TOE Security Assurance Requirements

The assurance requirements for the TOE are as specified in the EAL 2 package. This level was chosen considering the intended operational security environment for the TOE and the existing assurance measures in the development environment. The assurance requirements are summarized in Table 5-3. As none of the IT security assurance requirements are refined, they are not transcribed in the ST. The reader is referred to Part 3 of the Common Criteria. It should be noted that AVA_SOF.1 is not required for this evaluation as the password functionality is provided by IT environment.

Table 5.3: Security Assurance Components

Component	Component Name	Refined?
ACM_CAP.2	Configuration items	No
ADO_DEL.1	Delivery procedures	No
ADO_IGS.1	Installation, generation, and start-up procedures	No
ADV_FSP.1	Informal functional specification	No
ADV_HLD.1	Descriptive high-level design	No
ADV_RCR.1	Informal correspondence demonstration	No
AGD_ADM.1	Administrator guidance	No
AGD_USR.1	User guidance	No
ATE_COV.1	Evidence of coverage	No

Component	Component Name	Refined?
ATE_FUN.1	Functional testing	No
ATE_IND.2	Independent testing – sample	No
AVA_VLA.1	Developer vulnerability analysis	No

5.7 Strength of Function Requirement

There is no claimed strength of function (SOF) for the TOE. The user authentication password is required at the OS level only. The reader is referred to the Red Hat Linux AS version 3 update 3 security target for the SOF explanation.

5.8 Security Requirements for the IT Environment

The following security functions have been allocated to the IT environment.

5.8.1 Subset Access Control (FDP_ACC.1) (2)

FDP_ACC.1.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] on [assignment: processes acting on behalf of users as subjects and the following objects: files, directories and devices] and all operations among subjects and objects covered by the Discretionary Access Control Policy.

5.8.2 Security Attribute based Access Control (FDP_ACF.1) (2)

FDP_ACF.1.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to objects based on the following:

a) ***user identity; and***
b) ***ACLs and permission bits (read, write, execute)***.

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

File system objects within the ext3 file system:
A subject must have search permission for every element of the pathname and the requested access for the object. A subject has a specific type access to an object if:
The subject has been granted access according to the ACL_USER_OBJ or ACL_OTHER type entry in the ACL of the object.

Or

The subject has been granted access by an ACL_USER, ACL_GROUP_OBJ or ACL_GROUP entry and the associated right is also granted by the ACL_MASK entry of the ACL if the ACL_MASK entry exist.

Or

The subject has been granted access by the ACL_GROUP_OBJ entry and no ACL_MASK entry exists in the ACL of the object.

File system objects in other file systems:
A subject must have search permission for every element of the pathname and the requested access for the object. A subject has a specific type access to an object if:
The subject has the effective userid of the owner of the object and the requested type of access is within the permission bits defined for the owner.

Or

The subject has not the effective userid of the owner of the object but the effective group id identical to the file system objects group id and the requested type of access is within the permission bits defined for the group.

Or

The subject has neither the effective userid of the owner of the object nor is the effective group id identical to the file system object group id and requested type of access is within the permission bits defined for "world".

FDP_ACF.1.3 The TSF shall explicitly authorize access of subject to objects based on the following additional rules:

A process with a user ID of 0 is known as a root user process. These processes are generally allowed all access permissions. But if a root user process requests execute permission for a program (as a file system object), access is granted only if execute permission is granted to at least one user.

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules:

Write access to file system objects on a file system mounted as read-only is always denied. Write access to a file marked as immutable is always denied.

5.8.3 Basic Internal Transfer Protection (FDP_ITT.1)

FDP_ITT.1.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to prevent the [selection: disclosure, modification] of user data when it is transmitted between physically separated parts of the TOE.

5.8.4 User Authentication Before Any Action (FIA_UAU.2)

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.

5.8.5 User Identification Before Any Action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

5.8.6 Management of Security Attributes (FMT_MSA.1) (2)

FMT_MSA.1.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to restrict the ability to [selection: modify [assignment: no other operations]] the [assignment: access control attributes associated with a named object] to [assignment: administrative users and the owner of the object].

5.8.7 Static Attribute Initialization (FMT_MSA.3) (2)

FMT_MSA.3.1 The TSF shall enforce the [assignment: Discretionary Access Control Policy] to provide restrictive default values for security attributes that are used to enforce the Discretionary Access Control Policy.

FMT_MSA.3.2 The TSF shall allow the [assignment: administrative users and the owner of the object] to specify alternative initial values to override the default values when an object or information is created.

5.8.8 Specification of Management Functions (FMT_SMF.1) (2)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions [assignment: object security attributes management, user attribute management, authentication data management, audit event management].

5.8.9 Security Management Roles (FMT_SMR.1) (2)

FMT_SMR.1.1 The TSF shall maintain the roles: [assignment: authorized administrator, users authorized by the Discretionary Access Control Policy to modify object security attributes and users authorized to modify their own authentication data].

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

5.8.10 Internal TOE TSF data transfer (FPT_ITT.1)

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

5.8.11 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.8.12 Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that the TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.8.13 TSF Domain Separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

6. TOE SUMMARY SPECIFICATION

6.1 Statement of TOE Security Functions

This section contains a listing of the TOE security functions that satisfy the SFRs.

ITSF_AUDIT

The audit function records log file contents in a file. Viewing of the log files is restricted to the Primary Cluster Administrator. The following audit events are recorded:

- userok: Request from bad port (<port_number>)
- userok: Forged username suspected from <host/<port>

- resControl: Operation permission denied, uid = <uid)

In addition to the above listed events the audit function will record all write and execute operations on the following:

- Configure a cluster;
- Control (start and shutdown) of a cluster;
- Control (open and close) a queue;
- Submit a job;
- Control (suspend, resume, terminate and change a priority of a job);
- Add, configure and delete a host;
- Control (open and close) a host.

ITSF_ACCESS_CONTROL_POLICY

The TOE enforces a role based access control policy on subjects and objects based on defined roles. An access request is granted or denied based on a set of configuration files that define user-to-role and role-to-authorization mappings. The Primary Cluster Administrator is responsible for assigning users to roles. The TOE maintains the following roles:

- **Primary Cluster Administrator** – This is the first cluster administrator specified during installation and the first administrator listed in the lsf.cluster.cluster_name file. The Primary Cluster Administrator account owns the configuration and log files. The Primary Cluster Administrator has permission to perform cluster wide operations, change configuration files, re-configure the cluster and control jobs submitted by all users.
- **Cluster Administrator** – The cluster administrator may be specified during installation of configured after installation. Cluster administrators can perform administrative operations on all jobs and queues in the cluster. Cluster administrators have the same cluster wide privileges as the Primary Cluster Administrator except that they do not have permission to change LSF configuration files.
- **Queue Administrator** – The LSF Queue Administrator account has administrative permissions limited to a specified queue. The LSF queue administrator can perform operations on a specified queue, or on jobs running in the specified queue, but cannot change the LSF configuration or operate on LSF daemons.
- **Queue User** – They are any valid Operating System (OS) users who have permission to submit jobs to the LSF cluster.
- **User** – Any valid OS user.

Three basic rules are required to enforce the role based access control policy:

- **Role assignment** - A subject can access an object only if the subject has been assigned a role.

- **Role authorization** - A subject's active role must be authorized for the subject. This rule ensures that users can take on only roles for which they are authorized.
- **Operation authorization** - A subject can access an object only if the object is authorized for the subject's role.

The following tables outline the TOE's Role Based Access Control Policy.

Objects	Access Methods	Permission Categories		
		Read(R)	Write(W)	Execute(X)
Cluster	View cluster status and configuration	x		
	Configure a cluster		x	
	Control (start and shutdown) a cluster			X
Queue	View queue status and configuration	x		
	Add, configure, and delete a queue		x	
	Control (open and close) a queue			X
Job	View job status	x		
	Submit a job		x	
	Control (suspend, resume, terminate, and change priority of) a job			X
Host	View host status	x		
	Add, configure, and delete a host		x	
	Control (open and close) a host			X

Object	Primary Cluster Administrator	Cluster Administrator	Queue Administrator	Queue User	Any User
Cluster	RWX in a cluster	RX in a cluster	R in a cluster	R in a cluster	R in a cluster
Queue	RWX in a cluster	RX in a cluster	R in a cluster X in a queue	R in a cluster	R in a cluster
Job	RWX in a cluster	RWX in a cluster	R in a cluster WX in a queue	R in a cluster W in a queue X on own jobs	R in a cluster
Host	RWX in a cluster	RX in a cluster	R in a cluster	R in a cluster	R in a cluster

ITSF_ADMIN

The TOE provides functionality that enables an authorized user to effectively manage the TOE and its security functions. The Primary Cluster Administrator owns the configuration and log files. The Primary Cluster Administrator is the only user with the full permissions to perform cluster-wide operations – change configuration files and reconfigure the cluster; start and shutdown a cluster; open and close a queue; suspend, resume, terminate, and change priority of

any job in the cluster; and open and close a host. The Primary Cluster Administrator role is the only authorized role permitted to enforce and/or change resource allocation limits.

The Cluster Administrator can do cluster-wide administration based on existing configuration – start and shutdown a cluster; open and close a queue; suspend, resume, terminate, and change priority of any job in the cluster; and open and close a host. But the Cluster Administrator cannot change any configuration.

The Queue Administrator can do administration in a queue based on existing configuration – open and close the queue; suspend, resume, terminate, and change priority of any job in the queue. But the Queue Administrator can neither change any configuration, nor do any administration in the other queues.

ITSF_RESOURCE_ALLOCATION

Resource allocation limits are enforced on the following resources:

- Job slots by host,
- Job slots by processor,
- Memory,
- Swap space,
- tmp space, and
- Software licenses
- CPU time limit

Resource allocation limits apply to users and user groups, hosts and host groups, queues and all jobs in the cluster.

6.2 Statement of Assurance Measures

The following assurance measures are applied to satisfy the Common Criteria EAL2 assurance requirements.

- Configuration Management Assurance;
- Delivery and Guidance;
- Design Documentation;
- Tests; and
- Vulnerability Assessment.

Table 6.1: Security Assurance Components

Assurance Measures	Rationale
AM_ACM_CAP	A configuration management system for the development process is used and this is documented in the *Platform LSF HPC 6.2 Configuration Management Document* indicating that the TOE was developed using this CM system.
AM_ADO_DEL	Secure delivery procedures are documented in the *Platform LSF HPC 6.2 Secure Delivery And Operation Procedures*
AM_ADO_IGS	Installation procedures to securely install the TOE are provided in the *Installation and Setup for Platform LSF HPC 6.2: Common Criteria Evaluated Configuration*. A secure mode of operation is described to ensure the TOE is operating in secure mode.
AM_ADV_FSP	A functional specification document entitled *Platform LSF HPC 6.2 Security Functional Specification* is provided that describes each security function in the ST. External interfaces are described along with functional behavior at these interfaces. Error and exception handling is also described.
AM_ADV_HLD	The *Platform LSF HPC 6.2 Functional Security High Level Design* document is provided that describes the TOE functionality in subsystems. Interfaces are also described.
AM_ADV_RCR	The *Platform LSF HPC 6.2 Representation Correspondence* document is provided that maps the functions in the high level design to the functional specification and from the functional specification to the TOE summary specification.
AM_AGD_ADM	Administrator's manuals are provided that indicates the administrator's role and services. These documents are entitled *Administering Platform LSF 6.2, Using Platform LSF HPC 6.2, Installation and Setup for Platform LSF HPC 6.2: Common Criteria Evaluated Configuration, Using Platform LSF Multi-Cluster* and *Platform LSF Reference Version 6.2.*

Assurance Measures	Rationale
AM_AGD_USR	User manuals are provided that indicates the user's role and services. These documents are entitled *Platform LSF 6.2 Reference; Running Jobs on Platform LSF 6.2, Using Platform LSF HPC 6.2 and Installation and Setup for Platform LSF HPC 6.2: Common Criteria Evaluated Configuration.*
AM_ATE_COV	The *Platform LSF HPC 6.2 Test Coverage* document is provided that maps the tests done during development to the functional requirements in the ST.
AM_ATE_FUN	The *Platform LSF HPC 6.2 Common Criteria Test Plan* document contains the test plan and test cases that test each of the security functions in the ST are provided.
AM_ATE_IND	This is provided by the evaluation laboratory.
AM_AVA_SOF	This document is not required for this particular evaluation as the password functionality is provided by the IT environment.
AM_AVA_VLA	The *Platform LSF HPC 6.2 Vulnerability Assessment* document is provided that examines the TOE in its environment and indicates how the vulnerabilities are mitigated.

7. RATIONALE

This section demonstrates that TOE security functions and assurance measures are effective at solving the security problem defined for the environment in terms of threats, policies and assumptions. The approach is one of pair-wise refinement, whereby the stated security objectives are shown to be effective against the security problem, the security requirements are shown to satisfy the security objectives, and finally that the TOE summary specification is sufficient to meet the security requirements.

7.1 Security Objectives Rationale

This section demonstrates that the stated security objectives address all identified assumptions, threats, or policies. Table 7-1 demonstrates that each security objective covers at least one assumption, threat or policy, and that each assumption, threat and policy is covered by at least one security objective.

Table 7.1: Summary of Correspondence Between Threats /Policies and SO's for the TOE

Assumptions/Threats/Policies	O.ACCESS_CONTROL	O.AUDITING	O.ADMIN	O.AVAILABILITY
T.DENIAL_OF_SERVICE				X
T.ACCESS	X		X	
P.AUTHORIZED_USERS	X		X	
P.NEED_TO_KNOW	X			
P.ACCOUNTABILITY		X		

7.1.1 Security Objectives Sufficiency

This section demonstrates the sufficiency of the Security Objectives.

7.1.1.1 Threats

T.DENIAL_OF _SERVICE states that a TOE user or process could monopolize TOE resources thereby causing denial of service. This threat is countered by the **O.AVAILABILITY** objective which states that the TOE must provide functionality to control the use of resources by users and subjects such that a denial of service will not occur due to the monopolization of TOE resources.

T.ACCESS states that a TOE user could gain access to objects they are not permitted access to. This threat is countered by the **O.ACCESS _CONTROL** objective which states that the TOE must provide the means to enforce an access control policy among subjects and objects. This threat is also countered by the **O.ADMIN** objective which states that the TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

7.1.1.2 Policies

P.AUTHORIZED_USERS states that only those users who have been authorized to access the information within the system may access the system. This policy is addressed by the **O.ACCESS _CONTROL** objective which states that the TOE must provide the means to enforce an access control policy among subjects and objects. This policy is also countered by the **O.ADMIN** objective which states that the TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality.

P.NEED_TO_KNOW states that the system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a "need to know" for that information. This policy is addressed by **O.ACCESS _CONTROL** objective which states that the TOE must provide the means to enforce an access control policy among subjects and objects.

P.ACCOUNTABILITY states that the users of the system shall be held accountable for their actions within the system. This policy is addressed by the **O.AUDITING** objective which states the TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators.

Table 7.2: Summary of Correspondence Between Threats/Assumptions/Policies and SO's for the IT Environment

Assumptions/Threats/Policies	O..E.I_AND_A	O.E.DISCRETIONARY_ ACCESS	O.E.SECURE_CHANNEL	O.E.ENFORCEMENT	O.E.TIME_STAMPS	O.E.PHSYICAL	O.E_TRUSTED_ADMIN
A.TRUSTED_ADMIN							X
A.PHYSICAL						X	
T.E.TRANSIT			X				
T.E.ACCESS_TOE	X	X					
P.AUTHORIZED_USERS				X			
P.NEED_TO_KNOW				X			
P.ACCOUNTABILITY					X		

7.1.2 Security Objectives Sufficiency

This section demonstrates the sufficiency of the Security Objectives for the IT environment.

7.1.2.1 Assumptions

A.TRUSTED_ADMIN states that the system administrative personnel are trusted and not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the administrator/user documentation. Furthermore, the administrators of the TOE have been adequately trained in order for them to securely configure the TOE. This assumption is addressed by the **O.E.TRUSTED_ADMIN** objective which states those responsible for the management and configuration of the TOE must be trusted and adequately trained to perform their functions.

A.PHYSICAL states that the TOE resides in a controlled and physically secure environment. This assumption is addressed by the **O.E.PHYSICAL** objective which states that those responsible for the physical security of the TOE must ensure that the TOE is protected from physical attack.

7.1.2.2 Threats

T.E.TRANSIT states that data transferred between nodes is disclosed to or is modified by an authorized user or process. This threat is countered by the **O.E.SECURE _CHANNEL** objective which states that the IT environment must provide the means to transmit authentication data and user data securely to remote hosts.

T.E.ACCESS_TOE states that an unauthorized user gains access to the underlying OS, thereby gaining unauthorized access to the TOE. This threat is countered by **O.E.I_AND_A** which states that the IT environment must provide the means to identify and authenticate users of the TOE. This threat is also countered by **O.E.DISCRETIONARY_ACCESS** which states that the IT environment must control access to resources based on identity of users.

7.1.2.3 Policies

P.AUTHORIZED_USERS states that only those users who have been authorized to access the information within the system may access the system. This policy is supported by the **O.E. ENFORCEMENT** objective which states that the underlying OS (IT environment) must be designed and implemented in a manner which ensures that the organizational policies are enforced.

P.NEED_TO_KNOW states that the system must limit the access to, modification of, and destruction of the information in protected resources to those authorized users which have a “need to know” for that information. This policy is supported by the **O.E.ENFORCEMENT**

objective which states that the underlying OS (IT environment) must be designed and implemented in a manner which ensures that the organizational policies are enforced.

P.ACCOUNTABILITY states that the users of the system shall be held accountable for their actions within the system. This policy is supported by the **O.E.TIME_STAMPS** objective which states that the IT environment must provide reliable time-stamps for the audit records.

7.1.3 Security Requirements Rationale

This section demonstrates that the set of security requirements is suitable to meet the set of security objectives and is traceable to the set of security objectives.

Table 7.3: Security Requirements Rationale For the TOE

Function	O.ACCESS_CONTROL	O.AUDITNG	O.ADMN	O.AVAILABILITY
FAU_GEN.1		X	X	
FAU_SAR.1		X	X	
FAU_SAR.2		X	X	
FDP_ACC.1 (1)	X			
FDP_ACF.1 (1)	X			
FMT_MSA.1 (1)			X	
FMT_MSA.3 (1)			X	
FMT_MTD.1			X	
FMT_SMF.1 (1)			X	
FMT_SMR.1 (1)			X	
FRU_RSA.1				X

The following paragraphs demonstrate that the identified security requirements are appropriate to meet the security objectives.

O.ACCESS _CONTROL states that the TOE must provide the means to enforce an access control policy among subjects and objects. This objective is satisfied by the following SFRs:

- **FDP_ACC.1 (1) –** This SFR is used to determine the scope and set the parameters for the Role Based Access Control Policy.

- **FDP_ACF.1 (1) -** This SFR requires an access control policy which is based on specific attributes. An access control policy is enforced for the following roles: Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue user and Any User roles.

O.AUDITING states that the TSF must record the security relevant actions of users of the TOE. The TSF must present this information to authorized administrators. This objective is satisfied by the following SFRs:

- **FAU_GEN.1 -** This SFR requires that the TOE be able to generate an audit record of auditable events. The TOE monitors the following events :
  - userok: Request from bad port (<port_number>)
  - userok: Forged username suspected from <host/<port>
  - resControl: Operation permission denied, uid = <uid)

  The audit function will record all write and execute operations on the following:
  - Configure a cluster;
  - Control (start and shutdown) of a cluster;
  - Control (open and close) a queue;
  - Submit a job;
  - Control (suspend, resume, terminate and change a priority of a job);
  - Add, configure and delete a host;
  - Control (open and close) a host.

  The TOE records the above information in an audit log.

- **FAU_SAR.1 -** This SFR provides the Primary Administrator with the capability to read all the information recorded in the audit log. It also ensures that the audit records are recorded in a manner suitable for the Primary Administrator to interpret.

- **FAU_SAR.2 -** This SFR ensures that only the Primary Administrator has access to the audit files.

O.ADMIN states that the TOE must provide functionality, which enables an authorized administrator to effectively manage the TOE and its security functions, and must ensure that only authorized administrators are able to access such functionality. This objective is satisfied by the following SFRs:

- **FAU_GEN.1-** This SFR requires that the TOE be able to generate an audit record of auditable events. The TOE monitors the following events:
  - userok: Request from bad port (<port_number>)
  - userok: Forged username suspected from <host/<port>
  - resControl: Operation permission denied, uid = <uid)

  The audit function will record all write and execute operations on the following:
  - Configure a cluster;
  - Control (start and shutdown) of a cluster;
  - Control (open and close) a queue;
  - Submit a job;
  - Control (suspend, resume, terminate and change a priority of a job);
  - Add, configure and delete a host;
  - Control (open and close) a host.

The TOE records this information in an audit log.

- **FAU_SAR.1 –** This SFR provides the Primary Cluster Administrator with the capability to read all the information recorded in the audit log. It also ensures that the audit records are recorded in a manner suitable for the Primary Administrator to interpret.

- **FAU_SAR.2 –** This SFR ensures that only the Primary Cluster Administrator has access to the audit files.

- **FMT_MSA.1 (1) –** This SFR ensures that only the Primary Cluster Administrator can change, query, modify and delete the defined security attributes associated with the Role Based Access Control Policy.

- **FMT_MSA.3 (1)** – This SFR ensures that the access control policy default security attributes are restrictive in nature and that only the Primary Cluster Administrator has the ability to override the initial default settings.

- **FMT_MTD.1** – This SFR ensures that only the Primary Cluster Administrator has the ability to modify and delete the TOE configuration files.

- **FMT_SMF.1 (1) -** This SFR specifies the security functions provided to the Primary Cluster Administrator.

- **FMT_SMR.1 (1)** – This SFR requires that the TOE support roles. The following roles are supported: Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue User, Any User.

O.AVAILABILITY states that the TOE must provide functionality to control the use of resources by users and subjects such that a denial of service will not occur due to the monopolization of TOE resources. This objective is satisfied by the following SFR:

- **FRU_RSA.1 –** This SFR requires that the TOE enforce maximum quotas on resources. Resource allocation limits are enforced on the following resources:
  - Job slots by host,
  - Job slots by processor,
  - Memory,
  - Swap space,
  - tmp space, and
  - Software licenses
  - CPU time limit

  Resource allocation limits apply to users and user groups, hosts and host groups, queues and all jobs in the cluster.

Table 7.4: Security Requirements Rationale for the IT Environment

Function	O.E.I_AND_A	O.E.DISCRETIONARY_ACCESS	O.E.SECURE_CHANNEL	O.E.ENFORCEMENT	O.E.TIME_STAMPS
FDP_ACC.1 (2)		X			
FDP_ACF.1 (2)		X			
FDP_ITT.1			X		
FIA_UAU.2	X				
FIA_UID.2	X				
FMT_MSA.1 (2)		X			
FMT_MSA.3 (2)		X			
FMT_SMF.1 (2)		X			
FMT_SMR.1 (2)		X			
FPT_ITT.1			X		

Function	O.E.I_AND_A	O.E.DISCRETIONARY_ACCESS	O.E.SECURE_CHANNEL	O.E.ENFORCEMENT	O.E.TIME_STAMPS
FPT_STM.1					X
FPT_RVM.1				X	
FPT_SEP.1				X	

The following paragraphs demonstrate that the identified security requirements allocated to the environment are appropriate to meet the security objectives for the environment.

O.E.I_AND_A states that the IT environment must provide the means to identify and authenticate users of the TOE. This objective is satisfied by the following SFRs:

- **FIA_ UAU.2** - This SFR requires that users are to be successfully authenticated before any actions are taken on behalf of that user.

- **FIA_UID.2** – This SFR requires that each user identify themselves before allowing any other actions on behalf of that user.

O.E.SECURE _CHANNEL states that the IT environment must provide the means to transmit authentication data and user data securely to remote hosts. This objective is satisfied by the following SFRs:

- **FDP_ITT.1 –** This SFR requires that IT environment enforce a Discretionary Access Control Policy to prevent the disclosure, modification of user data when it is transmitted between physically separated parts of the TOE.

- **FPT_ITT.1 –** This SFR requires that the IT environment shall protect TSF data from disclosure, modification when it is transmitted between separate parts of the TOE.

O.E.DISCRETIONARY_ACCESS states that the IT environment must control access to resources based on identity of users. This objective is satisfied by the following SFRs:

- **FDP_ACC.1 (2) –** This SFR requires that the IT environment enforce a Discretionary Access Control Policy with a defined scope of control.

- **FDP_ACF.1 (2) –** This SFR requires the IT environment define and enforce the rules of the Discretionary Access Control Policy.

- **FMT_MSA.1 (2)** – This SFR requires that the IT environment must provide authorized users the ability to control who has access to objects.

- **FMT_MSA.3 (2)** – This SFR requires that the IT environment provide continuous protections of named objects starting from object creation.

- **FMT_SMF.1 (2)** – This SFR requires that aspects that need to be managed must be defined.

- **FMT_SMR.1 (2)** – This SFR requires that the IT environment provide the mechanism for an administrative user to manage the TOE.

O.E_ENFORCEMENT states that the underlying OS (IT environment) must be designed and implemented in a manner which ensures that the organizational policies are enforced. This objective is satisfied by the following SFRs:

- **FPT_RVM.1** – This SFR meets the objective by requiring that the TOE provide the means to ensure that security policy enforcement is not bypassed.

- **FPT_SEP.1 –** This SFR meets the objective by requiring that the TOE security functions are provided in a separate operating space that is not accessible by untrusted subjects

O.E_TIME_STAMPS states that the IT environment must provide reliable time-stamps for the audit records. This objective is satisfied by the following SFR:

- **FPT_STM.1 –** This SFR ensures that the IT environment can provide reliable time stamps, which will record the timing of security relevant events contained in the audit log.

7.2 TOE Summary Specification Rationale

The table below demonstrates the correspondence between the TOE SFRs and the summary specification of the TSF. All security functional requirements are addressed by at least one TSF, and the need for each TSF can be attributed to at least one SFR. Detailed descriptions of the TSFs can be found is Section 6.1.

Table 7.5: Summary of Correspondence Between the TSF and SFRs

Function	ITSF_AUDIT	ITSF_ACCESS_CONTROL_POLICY	ITSF_ADMIN	ITSF_RESOURCE_ALLOCATION
FAU_GEN.1	X			
FAU_SAR.1	X			
FAU_SAR.2	X			
FDP_ACC.1 (1)		X		
FDP_ACF.1 (1)		X		
FMT_MSA.1 (1)			X	
FMT_MSA.3 (1)			X	
FMT_MTD.1			X	
FMT_SMF.1 (1)			X	
FMT_SMR. 1 (1)			X	
FRU_RSA.1				X

7.2.1 IT Security Functions Rationale (SFRs)

The following table provides a coverage mapping to describe how the TOE Security Functions cover the SFRs.

Table 7.6: TOE Security Functions Rationale

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
FAU_GEN.1	ITSF_AUDIT	It is required that the TOE generates an audit record of specific events and record within each audit record specific details. This is covered in the audit functionality of the TOE which records log file

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		contents in a file.
FAU_SAR.1	ITSF_AUDIT	It is required that the Primary Cluster Administrator be able to read all the audit information from the audit record and that the audit records are provided in a manner suitable to interpret the information. ITSF_AUDIT details that the TOE records log file contents in a file.
FAU_SAR.2	ITSF_AUDIT	It is required that viewing of the log file be restricted to users that have been granted explicit access. ITSF_AUDIT provides the Primary Cluster Administrator with such access.
FDP_ACC.1 (1)	ITSF_ACCESS_CONTROL_POLICY	It is required that the TOE enforces a role based access control policy. The TOE implements a role based access control policy which permits subject access to resources based on predefined roles.
FDP_ACF.1 (1)	ITSF_ACCESS_CONTROL_POLICY	It is required that the TOE enforces the role based access control policy based on assigned subject and information security attributes.
FMT_MSA.1 (1)	ITSF_ADMIN	It is required that the management of security attributes is restricted to authorized users (Primary Cluster Administrator).
FMT_MSA.3 (1)	ITSF_ADMIN	This SFR ensures that only the Primary Cluster Administrator can change, query, modify and delete the configuration of the defined security attributes associated with the Role Based Access Control Policy.
FMT_MTD.1	ITSF_ADMIN	It is required that the TOE provide functionality to manage the TSF data. The Primary Cluster Administrator is responsible and is provided the functionality for managing the TOE configuration files.
FMT_SMF.1 (1)	ITSF_ADMIN	It is required that the TOE provide functionality to manage the TSF. The Primary Cluster Administrator is responsible and is provided the functionality for managing the audit management function, resource allocation function and the role based access control

Security Functional Requirement	TOE Security Function	TOE Security Function Mapped to SFR
		function.
FMT_SMR. 1 (1)	ITSF_ADMIN	It is required that the TOE supports roles. The TOE supports the following roles: Primary Cluster Administrator, Cluster Administrator, Queue Administrator, Queue User, Any User.
FRU_RSA.1	ITSF_RESOURCE_ALLOCATION	It is required that the TOE enforces maximum quotas on resources. Resource allocation limits are enforced on the following resources: ➢ Job slots by host, ➢ Job slots by processor, ➢ Memory, ➢ Swap space, ➢ tmp space, and ➢ Software licenses ➢ CPU time limit Resource allocation limits apply to users and user groups, hosts and host groups, queues and all jobs in the cluster.

7.3 Assurance Measures Rationale

Table 7-4 demonstrates the correspondence between the TOE SARs and the assurance measures. It illustrates that all security assurance requirements are addressed by at least one assurance measure, and the need for each assurance measure can be attributed to at least one SAR.

Table 7.7: Assurance Measures Rationale

Assurance Component	Assurance Measure	Rationale
ACM_CAP.2	AM_ACM_CAP	A configuration management system for the development process is used and this is documented indicating that the TOE was developed using this CM system.
ADO_DEL.1	AM_ADO_DEL	Secure delivery procedures are documented.

Assurance Component	Assurance Measure	Rationale
ADO_IGS.1	AM_ADO_IGS	Installation procedures to securely install the TOE are provided. A secure mode of operation is described to ensure the TOE is operating in secure mode.
ADV_FSP.1	AM_ADV_FSP	A functional specification document is provided that describes each security function in the ST. External interfaces are described along with functional behavior at these interfaces. Error and exception handling is also described.
ADV_HLD.1	AM_ADV_HLD	A document is provided that describes the TOE functionality in subsystems. Interfaces are also described.
ADV_RCR.1	AM_ADV_RCR	A document is provided that maps the functions in the high level design to the functional specification and from the functional specification to the TOE summary specification.
AGD_ADM.1	AM_AGD_ADM	A user manual is provided that indicates the administrator's role and services.
AGD_USR.1	AM_AGD_USR	A user manual is provided that indicates the user's role and services.
ATE_COV.1	AM_ATE_COV	A coverage document is provided that maps the tests completed during development to the functional requirements in the ST.
ATE_FUN.1	AM_ATE_FUN	A test plan and test cases that test each of the security functions in the ST are provided.
ATE_IND.2	AM_ATE_IND	This is provided by the evaluation laboratory.
AVA_VLA.1	AM_AVA_VLA	A vulnerability assessment is provided that examines the TOE in its environment and indicates how the vulnerabilities are mitigated.

Platform™

ANNEX "A"

GLOSSARY

A.1 Common Criteria Terminology

This section contains only those terms that are used in a specialized way in the CC. The majority of terms in the CC are used either according to their accepted dictionary definitions or commonly accepted definitions found in ISO security glossaries or other well-known collections of security terms.

Assets

Information or resources to be protected by the countermeasures of a TOE.

Assignment

The specification of an identified parameter in a component.

Assurance

Grounds for confidence that an entity meets its security objectives.

Attack potential

The perceived potential for success of an attack, should an attack be launched, expressed in terms of an attacker's expertise, resources and motivation.

Augmentation

The addition of one or more assurance component(s) from ISO 15408 Part 3 to an EAL or assurance package.

Authentication data

Information used to verify the claimed identity of a user.

Authorized user

A user who may, in accordance with the TSP, perform an operation.

Component

The smallest selectable set of elements that may be included in a PP, an ST, or a package.

Dependency

A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.

Evaluation Assurance Level (EAL)

A package consisting of assurance components from ISO 15408 Part 3 that represents a point on the CC predefined assurance scale.

Extension

The addition to an ST or PP of functional requirements not contained in Part 2 and/or assurance requirements not contained in ISO 15408 Part 3 of the CC.

Human user

Any person who interacts with the TOE.

Identity

A representation (e.g. a string) uniquely identifying an authorized user, which can be the full or abbreviated name of that user or a pseudonym.

Internal communication channel

A communication channel between separated parts of the TOE.

Internal TOE transfer

Communication of data between separated parts of the TOE.

Object

An entity within the TSC that contains or receives information and upon which subjects perform operations.

Organizational Security policies

One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations.

Package

A reusable set of either functional or assurance components (e.g. an EAL), combined together to satisfy a set of identified security objectives.

Protection Profile (PP)

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Refinement

The addition of details to a component.

Role

A predefined set of rules establishing the allowed interactions between a user and the TOE.

Secret

Information that must be known only to authorized users and/or the TSF in order to enforce a specific SFP.

Security attribute

Information associated with subjects, users and/or objects that are used for the enforcement of the TSP.

Security Function (SF)

A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Function Policy (SFP)

The security policy enforced by an SF.

Security objective

A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions.

Security Target (ST)

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Selection

The specification of one or more items from a list in a component.

Strength of Function (SOF)

A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behavior by directly attacking its underlying security mechanisms.

SOF-basic

A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium

A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high

A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organized breach of TOE security by attackers possessing a high attack potential.

Subject

An entity within the TSC that causes operations to be performed.

Target of Evaluation (TOE)

An IT product or system, including its associated administrator and user guidance documentation, that is the subject of an evaluation.

TOE resource

Anything useable or consumable in the TOE.

TOE Security Functions (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

A set of rules that regulates how assets are managed, protected and distributed within a TOE.

TOE security policy model

A structured representation of the security policy to be enforced by the TOE.

Transfers outside TSF control

Communication of data to entities not under control of the TSF.

Trusted channel

A means by which a TSF and a remote trusted IT product can communicate with the necessary confidence to support the TSP.

Trusted path

A means by which a TSF and device physically separated from the TOE can communicate with the necessary confidence to support the TSP.

TSF data

Data created by and for the TOE, which might affect the operation of the TOE.

TSF Scope of Control (TSC)

The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

User

Any entity (human user, resident added application, or external IT entity) outside the TOE that interacts with the TOE.

User data

Data created by and for the user, which does not affect the operation of the TSF.

Copyright

7.3.1 Trademarks