Project Acronym:	**OPTIMIS**
Project Title:	**Optimized Infrastructure Services**
Project Number:	**257115**
Instrument:	**Integrated Project**
Thematic Priority:	**ICT-2009.1.2 – Internet of Services, Software and Virtualisation**

Provider's Risk Assessment Tools User Guide

Activity 3: *Service Deployment*

WP 3.4: *Provider's Risk Assessment Tools*

Due Date:		M34
Submission Date:		15/03/2013
Start Date of Project:		01/06/2010
Duration of Project:		36 months
Organisation Responsible for the Deliverable:		University of Leeds
Version:		1.0
Status		Final
Author(s):	Ming Jiang	ULEEDS
	Thomas Kirkham	ULEEDS
	Karim Djemame	ULEEDS

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission)	
RE	Restricted to a group specified by the consortium (including the Commission)	
CO	Confidential, only for members of the consortium (including the Commission)	

Version History

Version	Date	Comments, Changes, Status	Authors, contributors, reviewers
0.1	08/03/2013	First draft	Ming Jiang
1.0	15/03/2013	Final Version	Ming Jiang

Table of Contents

Index of Figures

1 Introduction

This document includes the user guide for the software component Provider's Risk Assessment Tools: Service Provider Risk Assessment Tool (SPRAT) and Infrastructure Provider Risk Assessment Tool (IPRA). The SPRAT is responsible for supporting the risk-aware negotiation with IPs on behalf of end-users. The IPRAT estimates risk for an SLA violation and supports the IP's decision of agreeing an SLA as well as of initiating fault-tolerance mechanisms to prevent SLA violation. Risk assessment conducted by IPRAT improves the IP's reliability and QoS.

1.1 Glossary of Acronyms

Acronym	Definition
AC	Admission Controller
APoF	Adjusted Probability of Failure
CO	Cloud Optimizer
FTE	Fault Tolerance Engine
HM	Holistic Manager
IPRAT	Infrastructure Provider Risk Assessment Tool
PoF	Probability of Failure
SDO	Service Deployment Optimizer
SPRAT	Service Provider Risk Assessment Tool
SLA	Service Level Agreement
VMM	Virtual Machine Manager

2 SPRAT User Guide

2.1 Release information

Component Name	Release Number	Release Date
Service Provider Risk Assessment Tool (SPRAT)	1.0-SNAPSHOT	15/03/2013

2.2 Introduction

The SP is responsible for supporting the risk-aware negotiation with IPs on behalf of end-users. Therefore, the SDO provides the functionality to rank SLA offers and present them to end-users, based on risk assessment obtained through interaction with a risk assessment module and possibly assessments received from IPs.

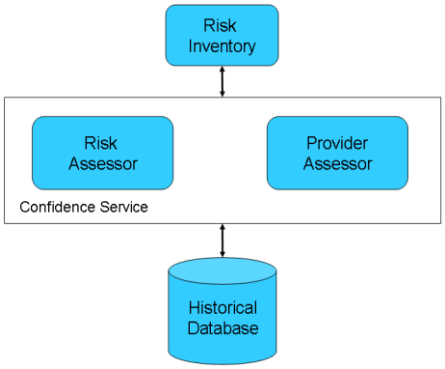

Figure 1 Service Provider – Risk Assessment Components

To support this functionality, a number of components are identified (see Figure 14): a Confidence Service, a risk module (comprising a Risk Assessor and a Risk Inventory), and a Historical Database. These are described below.

- Confidence Service

The SDO makes use of the confidence service to query and obtain risk estimation for IP's generated offers. Its role is to utilize statistical data relating to previous offers to estimate the reliability of the current IP's offer. The risk of exposure level is represented on a scale of 1-5: very low, low, medium, high, and very high. In order to compute the reliability information, the Confidence Service has a Risk Assessor component.

- Risk Assessor

This component uses the risk inventory and retrieves data from the historical database to estimate the risk associated with the IP's offer. Additionally it must be able to define a response (i.e. mitigation) strategy for the identified risks. Typical mitigation strategies are: retention, avoidance, reduction and transfer. Mitigation alternatives are determined for each type of incident (see risk inventory).

- Provider Assessor

The assessment of an IP by an SP is based on 7 criteria that are chosen from the high level risk perspectives and their sub-criteria that are either already widely available from the information sources of Cloud resources providers or being proposed by various Cloud bodies and guidelines such as NIST and ENISA for future Cloud providers to adopt:

1. Past SLA Performance: NumberSLASuccessful.
2. Geography Information: GeographicThreatLevel, PolicalStabilityLevel, JurisdictionTransparencyLevel, JurisdictionOverlappingLevel.
3. Certifications and Standards Compliance: FacilityRelatedCertificationLevel, OpertionRelatedCertificationLevel, HRRelatedCertificationLevel, IndustryStandardComplianceLevel.
4. Business Stability: BusinessHistoryInYears, EmployeeNumber, CustomerNumber.
5. General Infrastructure Practice: AvailableComputeResources, AvailableSpareResources, AverageNodeAvailability, StorageBackupFrequency.
6. General Security Practice: FacilitySecurityLevel.
7. General Privacy Practice: FacilityAndDataAccessControlLevel, PersonalDataProtectionLevel.

- Risk Inventory

This inventory is populated with Assets, Incidents/Risk Scenarios and Impact/Consequences, described below.

1. Assets: In the context of the SP, assets are the services to deploy. The SP (as well as the end-user) is sensitive to how the service is going to be deployed in terms of security, latency, or other service important characteristics such as cost and energy-efficiency. Hence, asset capacity, availability and their variability are of greater interest for the level of service provision desired. The service manifest places heavy emphasis on the service level provision characteristics. Asset characteristics relating to service provision are decomposed into areas of interest and those areas will be described in terms of indicators in order to be able to understand the weaknesses of the asset and its impact on the risk profile. Potential risk events are assessed in terms of these.
2. Incidents / Risk Scenarios refer to assets and combination of assets. An incident aims to describe any event, condition or their combination that has the potential to reduce the capacity or availability of an asset. Incidents are described in order to establish a minimum level of originality in the assessment. Therefore, the collection methodology will guarantee that the incidents modeled describe situations, which have occurred or could occur in reality. Incidents are composed of vulnerabilities, threats and adaptive capacity.
3. Impact/Consequences of a risk incident such as degraded performance, loss of data etc. These will be evaluated according to the indicators selected to describe the assets in step 1 and it will account for the costs associated with using the service as well as the costs of not meeting predefined service levels (in this case the re-deployment of the service may be necessary).
4. Historical database

   The database contains data necessary to estimate risks such as past SLA transactions (offers accepted, rejected etc).

2.3 Functionalities

- SPRAT's Stage 1 will involve the SDO invoking the SPRA to collect some basic data about the IP's available for use. After receiving this data from the monitoring tool, the SDO will then be able to request a risk factor of working with each of the IPs available.
- SPRAT's Stage 4 will involve the IP telling the SP about the risk it estimates of failure if the service is deployed on it. The SDO on the SP side will read in this detail and calculate an adjusted probability of failure (APoF) using its own historical data. The SDO will then make a decision on where to deploy the service.
- SPRAT's Stage 5 involves dynamic assessment of the service on the SP level.

2.4 Known limitations

2.5 Getting Started

See Section 2.6 of Provider's Risk Assessment Tools Installation Guide [1]

2.6 FAQ

2.7 Other information

2.7.1 Source Code Information

SVN Repository URL:

http://pandora.atosorigin.es/svn/optimis

Component Folder:

/branches/OptimisY3/ServiceProviderRiskAssessmentTool

2.7.2 Directory Structure

SVN Source Code Browser:

http://pandora.atosorigin.es/gf/project/optimis/scmsvn/

2.7.3 Contributors

- Mariam Kiran
- Ming Jiang

3 IPRAT User Guide

3.1 Release information

Component Name	Release Number	Release Date
Infrastructure Provider Risk Assessment Tool (IPRAT)	1.0-SNAPSHOT	15/03/2013

3.2 Introduction

Provider risk assessment increases the performance and quality of an IP. The estimated risk for an SLA violation supports the IP's decision of agreeing an SLA as well as of initiating fault-tolerance mechanisms to prevent SLA violation. Thus, risk assessment improves the IP's reliability and QoS.

When the SDO sends a service manifest in a request for quotes the AC evaluates the feasibility of admitting the new service, with respect to current infrastructure load, predicted future capacity, as well as risk. Also, when the SDO sends a deployment request, including the service manifest and the agreed offer to the IP, the IP determines where to place VMs by combining its local management policy with the functional and non-functional requirements specified in the service manifest. Again, this includes risk assessment. Figure 15 outlines the architectural components for the IP risk management.

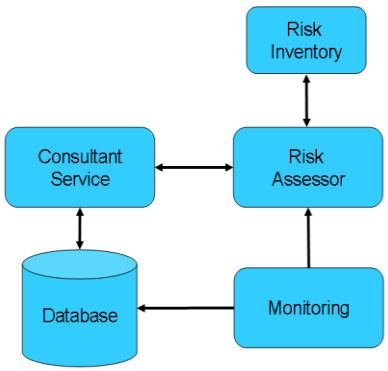

Figure 2 Infrastructure Provider – Risk Assessment Components

- Consultant service

The consultant service supports the risk assessor with statistics in order to estimate risk. To build these statistics, it has to provide data-mining methods on past events. The consultant service has access to all monitoring information available through the monitoring service. This data includes static and dynamic information about the IP's resources and services in operation. Examples of such information are current workload, system outages, temporary performance shortages, monitored network traffic, experts' availability, or general information regarding number of services to operate. Monitored data is also used to determine

bottlenecks in the IP's infrastructure so that the provider can improve its capacity planning, administration, and management of its resources. This leads to higher, cost-effective productivity of virtualised resources.

- Risk Assessor

The assessment of an SP by an IP is based on 3 criteria that are chosen from the high level risk perspectives and their sub-criteria that are either already widely available from the information sources of Cloud resources providers or being proposed by various Cloud bodies and guidelines such as NIST and ENISA for future Cloud providers to adopt:

1. Past SLA Performance: NumberSLASuccessful.
2. Business Stability: BusinessHistoryInYears, EmployeeNumber, CustomerNumber.
3. General Security Practice: FacilitySecurityLevel.

The risk assessor assesses different risks on static and dynamic data as well as on forecasts. This data is provided from the consultant service by collecting monitoring information and building statistics. With the use of risk assessment and data mining methods:

1. Admission Controller (AC) can assess the risk of fulfilling a given service manifest. It can use this information to optimize its offers as well as its scheduling strategy.
2. Holistic Manager (HM) can utilize the risk assessment information (e.g. PoF for the overall infrastructure and for individual components (network, VMs, storage, experts' support, backup, etc.)) to build up the whole state image of the system, decide or adjust the overall polices to be applied by the various low level VM Manager and Data Manager.
3. Data Manager can assess the dynamic changes in risk during service operation. Monitoring can detect significant changes and therefore the VM Manager and Data Manager, based on the policies defined by the CO, can decide to initiate fault-tolerance mechanisms, e.g. VM migration, initiation of precautionary replication of data.

If an incident is detected, the monitoring system sends an alert message to the risk assessor and initiates a risk mitigation strategy. This determines the impact on risk and allows the VM Manager and Data Manager to react accordingly.

- Monitoring

This component gathers all necessary runtime information that is collectable by sensors in the infrastructure and can predict or detect risky events. Early identification of risky events may increase the likelihood of the successful service operation.

- Risk Inventory

This inventory is populated with:

1. Assets. In the context of the IP, there are a large number of assets which include the services in operation, VMs, storage, network etc. The IP (as well as the SP) is sensitive to how the service is running in terms of security, performance, or other service important characteristics such as cost and energy-efficiency. Hence, asset capacity, availability and their variability are of greater interest for the level of service provision desired. Asset characteristics relating to service operation are decomposed into areas of interest and those areas will be described in terms of indicators in order to be able

to understand the weaknesses of the asset and its impact on the risk profile. Potential risk events are assessed in terms of these.

2. Incidents / Risk Scenarios. Here an incident aims to describe any event, condition or their combination that has the potential to reduce the capacity or availability of an asset, e.g. service in operation. Incidents are composed of vulnerabilities, threats and adaptive capacity and include for example a service failure, an increase in energy consumption, a security breach etc.

3. Impact/Consequences of a risk incident such as service degraded performance, loss of data etc. These will be evaluated according to the indicators selected to describe the assets in step 1 and will account for the costs associated with using the service as well as the costs of not meeting predefined service levels (in this case fault-tolerance mechanisms, migration of VMs, cloud bursting etc).

3.3 Functionalities

- IPRAT is able to collect some basic information about the SP in question. Using this information the IPRA can send results back to the AC to give an indication of the risk of working with that SP with the Probability of Failure (PoF) of the Service Manifest is to be deployed. This maps to stages 2 and 3 of risk assessment stages.
- IPRAT is able to conduct the dynamic assessment of the service during operation on the IP. During this phase the monitoring tool will be constantly observing the service collecting various data. This data will be read in by the IPRAT and returns the mitigation strategies to the HM and the Data Manger in case something goes wrong. This is mapped to the risk assessment stage 6.
- **Forecasting/'What If' (Tom)**

3.4 Known limitations

None

3.5 Getting Started

See Section 3.6 of Provider's Risk Assessment Tools Installation Guide [1]

3.6 FAQ

3.7 Other information

3.7.1 Source Code Information

SVN Repository URL:

http://pandora.atosorigin.es/svn/optimis

Component Folder:

/branches/OptimisY3/InfrastructureProviderRiskAssessmentTool

3.7.2 Directory Structure

SVN Source Code Browser:

http://pandora.atosorigin.es/gf/project/optimis/scmsvn/

3.7.3 Contributors

- Ming Jiang
- Thomas Kirkham

4 Risk in the TREC GUI

4.1 Release information

Risk at service runtime can be visualized using the TREC GUI. The TREC GUI is part of the wider IP dashboard and a separate document details the configuration and installation of the dashboard.

4.2 Introduction

Risk is part of the wider TREC metrics that can be visualized on the Dashboards. The TREC graphs can be accessed using the TREC tab on the GUI.

4.2.1 TREC

The TREC tab accesses the TREC GUI without specifying a particular level to be displayed. Note that when accessing the TREC GUI through the Cloud Optimizer tab, a particular level (service, infrastructure, node, VM) and a particular identifier (for service, node and VM levels) are already selected and fixed in the TREC GUI to avoid having to introduce them manually. By accessing the TREC GUI through this tab, you can access all the options of the TREC GUI and allows you to visualize information on services/VMs that are no longer running in the infrastructure.

The Risk Tab allows risk to be monitored for a specific service ID. This needs to be supplied along with the infrastructure ID that the services are running on

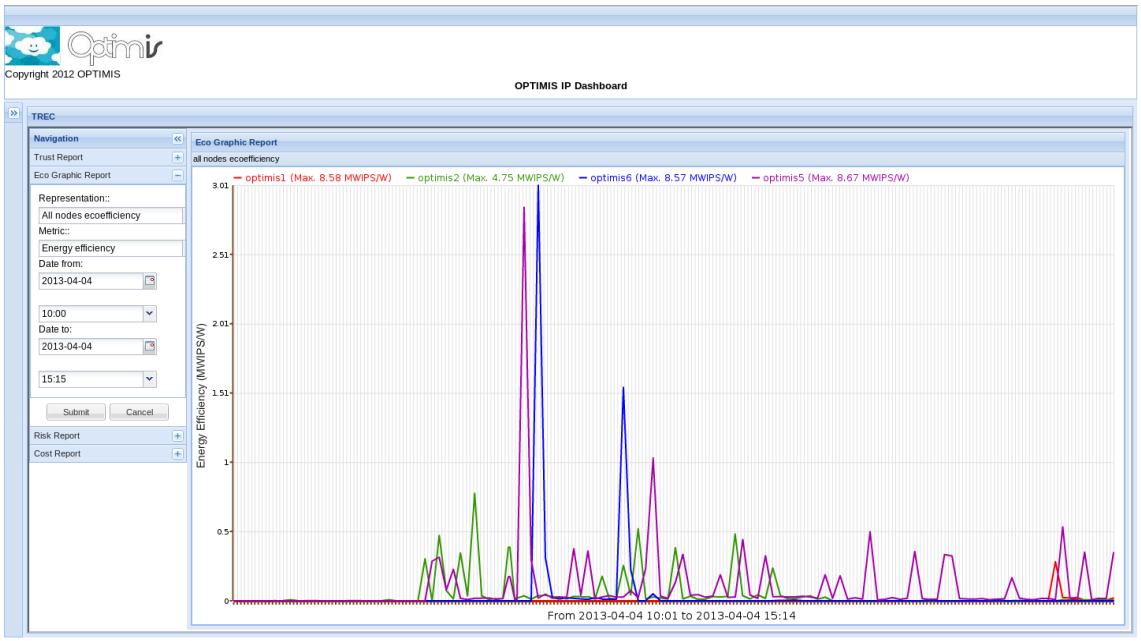

Figure 3 TREC GUI tab

4.3 Known limitations

N/A

4.4 Getting Started

4.4.1 Using the Software

To use the software, simply access to the IP Dashboard to get access to the trec GUI through a web browser through the following link:

http://IPVM_URL:PORT/IPManagerWeb

or you can access the TRECGUI directly using the link below

http://IPVM_URL:PORT/TrecgManagerWeb

4.4.2 Testing the Software

This component does not have a specific way to be tested. In fact, it is used to test the functionality of other components and display the information they produce. Therefore, as long as the different tabs display the required information it can be assumed that it is working properly.

4.4.3 Configuration

See the Installation Guides for the IP and SP Dashboards

4.5 FAQ

N/A

4.6 Other information

4.6.1 Source Code Information

The source code of the component is contained in a single folder and can be downloaded from the project's SVN using the following command:

svn co http://pandora.atosorigin.es/svn/optimis/branches/OptimisY3/IPManagerWeb IPManagerWeb/

The code is based on the Google Web Toolkit [1].

4.6.2 Directory Structure

The IP Dashboard uses two directories:

- *Configuration directory*: it contains the configuration files of the IP Dashboard. It is located at $OPTIMIS_HOME/etc/IPManagerWeb. An overview of the configuration files available is provided at the Installation Guide.
- *Output logs directory*: it contains the log files generated by the IP Dashboard. It is placed at $OPTIMIS_HOME/var/log/IPManagerWeb. There are three log files available:

- IPManagerWeb.log: contains all the messages emitted by the IP Dashboard, being “DEBUG” the minor level of all of them, including all the necessary details, such as time, message type, emitting class, thread, line, etc. To be used for low-level debugging purposes.
- IPManagerWeb_Simplified.log: it is a simplified version of the previous file, also containing from “DEBUG” messages upwards, but only displaying the time and the message type.
- IPManagerWeb_SimplifiedINFO.log: it only contains from “INFO” messages upwards, and only displays the time and message type of each of them.

4.6.3 Contributors

Josep Subirats (BSC)

Jordi Guitart (BSC)

Django Armstrong (Uleeds)

Tom Kirkham (ULeeds)

Ming Jiang (Uleeds)

5 References

[1] Google Web Toolkit webpage: https://developers.google.com/web-toolkit/

[2] Provider's Risk Assessment Tools Installation Guide.