COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

CIP-ICT-PSP-2013-7

SERVICE DISTRIBUTION NETWORK AND TOOLS FOR INTEROPERABLE PROGRAMMABLE, AND EXPLOITATION OF UNIFIED PUBLIC CLOUD SERVICES

Deliverable D4.1b

STRATEGIC Cloud Broker and Marketplace

Work package	WP4 – Framework Implementation, Integration, and Test
Editor(s):	Joshua Daniel, Géry Ducatel, Enric Page Montanera
Responsible Partner:	British Telecommunications
Quality Reviewers	Ilja Livenson, Nuria Rodriguez
Status-Version:	v1.0
Date:	06/11/2015
EC Distribution:	Public
Abstract:	This document describes the evolution of the Marketplace design and capabilities. The integration of an extension framework now enables delivery and management of common capabilities across multi-cloud deployments. This document describes the onboarding of horizontal security services to the STRATEGIC Service Store with an integrated consumer experience ensuring a workload's Life cycle is in sync with that of its security.

This project has received funding from the European Union's Competitiveness and Innovation Framework Programme under grant agreement no 621009

Document Revision History

Version	Date	Modifications Introduced	
		Modification Reason	**Modified by**
V0.1	03/08/2015	ToC & Abstract	BT
V0.2	18/08/2015	Introduction	ATOS
V0.3	27/08/2015	Marketplace Extension Security	BT
V0.4	01/09/2015	Marketplace Extension Trust	ATOS
V0.5	10/09/2015	Merge from previous versions	ATOS
V1.0	13/10/2015	Conclusions and internal review	ATOS & BT
V1.1	14/10/2015	Quality review process	NICPB
V1.2	06/11/2015	Final version for submission	ATOS

Contents

List of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym	Title
Administrator	Customer account administrator, typically, the user who has opened the account in the Marketplace.
API	Application Programmatic Interface: input and output channels into software products for interaction.
AWS	Amazon flagship virtualisation service (Amazon Web Service).
Cloud Broker	An application that allows end users to choose a cloud service on the basis of price and capabilities.
CloudPlatform	A Citrix private cloud interface software originally based on CloudStack.
CloudStack	An Apache licenced private cloud interface software which is the basis of CloudPlatform.
CRUD	Create Remove Update Delete. This refers to a user management interface .
CSV	Comma Separated Values. A file standard to save, and transfer platform independent data.
Developers	Software providers for the Marketplace.
IaaS	Infrastructure as a Service. A virtualisation technology that creates Virtual Machines loaded with an Operating System accessible remotely.
IMS (user store)	Identity Management Service. A user directory product in the Marketplace.
ISV	Independent Software Vendor.
KSM	Kernel-based Virtual Machine. A technology that allows the deployment of a hypervisor onto a Linux kernel. This allows the transformation of a standard Linux server into a low level virtualisation server.
LDAP	Lightweight Directory Access Protocol. A protocol to read and write information from a user database. Often used to also refer the said user database.
Marketplace	The Marketplace is the web based console users access to buy and sell services. The marketplace is the host of the Service Store.
Multi-cloud	The ability to target different cloud targets.
OpenStack	A private virtualisation software which was originally developed by Rackspace. OpenStack is Open Source under Apache licence.
OPTIMIS	A European project which focussed on optimisation tools for cloud brokering services.
OS	Operating System, e.g. Linux, Windows, etc…
OVA	Open Virtualisation Archive. A file that is used to save an entire Virtual Machine usually for backup, or transfer.
P2V	Physical to Virtual. A tool to create a Virtual Machine from an existing physical machine or server.
PaaS	Platform as a Service. A cloud computing service that provides access to software stacks and services.
Rackspace	A company that provides public cloud platform

Acronym	**Title**
	technology.
RDP	Remote Desktop Access. A Microsoft proprietary protocol to view and interface with a virtual machine.
REST	Representational State Transfer. An interoperability framework for web based applications. This is typically used for web consoles, or applications to obtain read and write access to an on-line service.
Server Template	A file that can be loaded to obtain a Virtual Machine manageable from a virtual interface console (such as the Marketplace).
Service Store	The service functions of the Marketplace.
STRATEGIC Administrators	Users that have access to the administrative console of the marketplace.
URL	Universal Resource Locator. Used to represent locations such as web addresses.
VMWare	A company selling low level virtualisation technology.
VMWare VCloud	A VMWare product for private cloud.
Windows Azure	A cloud computing platform from Microsoft providing IaaS, and PaaS.
Xen	A type of hypervisor provided Open Source under the GPL licence (General Public Licence)

Table 1: Definitions, Acronyms and Abbreviations

Executive Summary

The work carried out within WP4 integrates, tests and delivers STRATEGIC framework and associated cloud infrastructures. This work supports development of the pilot services and conduction of the pilot operations. The Service Store has been integrated with a managed services on boarding framework and the security services integration is delivered in an iterative fashion on the basis of the customization of background platforms and capabilities of the project, as well as on the basis of the design/integration of the added-value services of the STRATEGIC framework.

The deliverables "**D4.1a, D4.1b, D4.1c STRATEGIC Cloud Broker / Marketplace"** are a prototype and an accompanying report associated with the implementation of the STRATEGIC Cloud Broker, as well as with the establishment of the marketplace infrastructure of the project.

This is the second iteration of the D4.1 deliverable, detailing work that carried out since the publication of the first iteration. This document details and documents the user experience that will be delivered to the users of the STRATEGIC store when consuming the security services. An integration method using *micro-services* model was used to achieve the required level of synchronisation for the automation deployment and lifecycle management of the security services alongside the deployment of multi-server multi-tier applications from the Service Store. A common model for user journey has been achieved for the consumption of such services with the BT Intelligent Protection integration creating a precedent. The document also describes the integration work carried out to adapt the trust assessor component into STRATEGIC, which is in charge of the infrastructure provider assessment.

1 Introduction

1.1 Scope of the document

This document is the second iteration of the STRATEGIC Cloud Broker and Marketplace, previous iteration submitted at the end of the first year as "*D.4.1a Cloud Broker / Marketplace*". The document is the accompanying report associated with the implementation of the STRATEGIC Service Store, as well as with the establishment of the marketplace infrastructure. The second iteration describes the horizontal security services, which are available for the pilot operations run in WP5.

1.2 Target audiences

This report is intended for the following audiences:

a) Cloud Security Providers: The on-boarding framework for managed services described in this report, a.k.a. 'Horizontal services', formalises a new channel for delivering security services as an integrated and subscription based Cloud product.
b) STRATEGIC Service Store Users/Operators: The Horizontal service framework creates a new channel for integrating and syncing the lifecycle management of security, including security control injection, monitoring and enforcement, with that of the cloud products.
c) Pilots or Public Sector organizations: The Horizontal services enable seamless consumption of security services as a subscription based product with multi-cloud capability.

1.3 Structure of the document

The document is structured as follows:

- Chapter 1 introduces the content of the report, the audience and its structure; the report extends the first iteration of the Cloud Broker marketplace report delivered in Y1.
- Chapter 2 covers the horizontal security services integrated within the Service Store capabilities.
- Chapter 3 describes the integration work carried out to adapt the infrastructure provider reputation mechanism.

2 STRATEGIC Service Store Extension: Security

2.1 Extension Framework Overview

Security is a prime concern for cloud deployment as noted in the deliverable 4.1a. [3] Securing a product through its lifetime requires a capability that allows complete synchronisation of the security capability alongside to enable optimum visibility and control. As part of the STRATEGIC project, all the pilots are being offered Application & Host protection and Data protection, where both features are delivered as a service by BT.

However, as with any deployment security needs to be configured for each asset deployed to ensure that all the necessary protection rules are in place. This can be a very time consuming process and has scope for error to be made. With the STRATEGIC Service Store supporting multi-cloud deployments that are multi-tier in topology, enabling right level of security right at the time of deployment is a must. The Horizontal services framework is designed to address this very pain point.

2.2 Service Design Model

Both of the security services provided by BT that were integrated with STRATEGIC Service Store are subscription based and multi-tenant, where every customer is provisioned a corresponding tenant account. This tenant account allows access to a personalised dashboard to monitor and manage one's deployments.

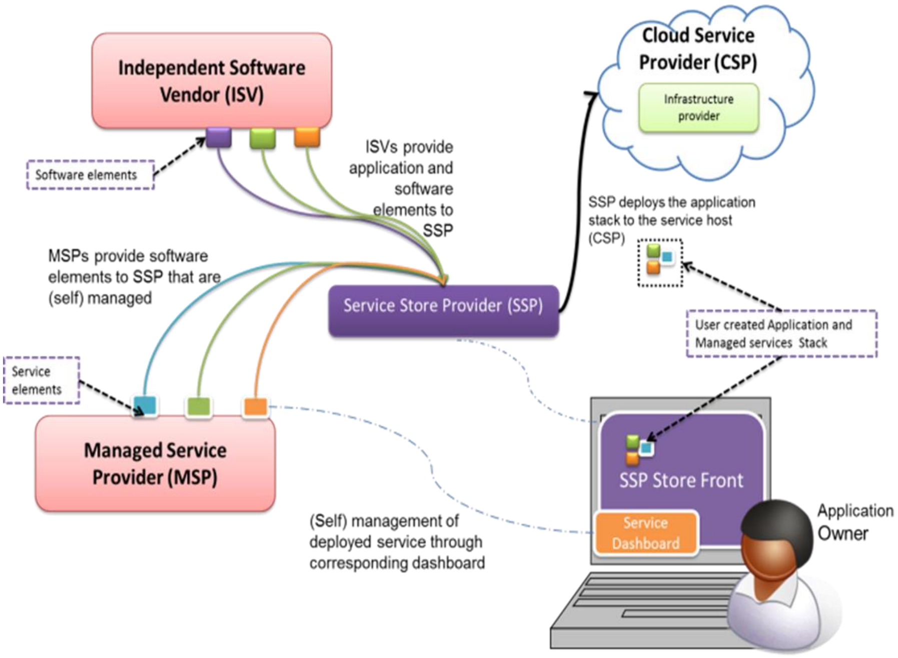

Independent Software Vendor (ISV)
Software elements
ISVs provide application and software elements to SSP
Cloud Service Provider (CSP)
Infrastructure provider
SSP deploys the application stack to the service host (CSP)
MSPs provide software elements to SSP that are (self) managed
Service Store Provider (SSP)
User created Application and Managed services Stack
Service elements
Managed Service Provider (MSP)
SSP Store Front
Service Dashboard
Application Owner
(Self) management of deployed service through corresponding dashboard

Figure 1: Depicting the Services integration architecture to integrate deployment and lifecycle management of security service provided by a Managed Security Provider.

Figure 1 depicts the interaction diagram between the Managed Services (security) with that of the deployment of applications from independent software vendors on a cloud environment by the user. The horizontal services integration framework of the STRATEGIC Service Store allows for re-configuration of deployed applications and injection of appropriate security controls into the deployment, which all can then be managed from a common dashboard.

With the goal of enabling the complete lifecycle management of these security services with the necessary configuration as seamless as possible, the following common sequence of service design was adopted:

1) A STRATEGIC Service Store user subscribes to a particular security service.
2) A corresponding tenant account is created on that security service upon request by the user.
3) The users are then able to enable various security modules that they wish to consume and update their account settings.
4) Depending on the security service type, the user is presented with a choice to enable a security service at a chosen level for a particular deployment during provisioning. The service store will then orchestrate the deployment and configuration of the requested security modules with the user specified configuration.
5) Once an application was launched, the security configurations for individual virtual machines can then be updated, or switched off, via the Workload management workflow in the STRATEGIC Service Store.
6) Finally, when an workload or a server is decommissioned the corresponding security service is removed from the asset and related information from the management server.
7) Upon unsubscribing from a security service, all the security is disable for that particular tenant from all their cloud assets.

The above described experience of subscription based consumption of managed services is referred to as Extension Services. The Extension Service framework is built on the concept of microservices. It encourages developers with different skill sets to provide additional functionalities to Service Store - Cloud Application Delivery and Management Platform. The extension services middleware created is then able to interact with the Service Store and hence orchestrate the lifecycle management of a specific extension service.

The term "Microservice Architecture" has sprung up over the last few years to describe a particular way of designing software applications as suites of independently deployable services. While there is no precise definition of this architectural style, there are certain common characteristics around organization around business capability, automated deployment, intelligence in the endpoints, and decentralized control of languages and data.

—Martin Fowler, author of Refactoring

Each extension service module provides a single business function to add on to STRATEGIC Service Store. As part of STRATEGIC project the two functions that have been onboarded to STRATEGIC Service Store as extension services are Application & Host protection and Data Encryption as a Service.

2.3 BT Intelligent Protection – User Journey

Extension services are subscription based services. A subscription can be optioned in by an organisation for services to apply to all users and deployments across their account. Extension services have been designed to provide consistent and homogenous service behaviour. This consistency allows organisations to enforce policies and business rules for compliance. Extension services are also configurable and flexible. An organisation can retrospectively enforce an extension service or remove it. The configuration of the service can also be modified after the initial deployment in order to tighten or loosen restriction rules and policies. Service administrators should use extension services to build secure and compliant services for end users.

When an extension service has been applied to an account, applications that are impacted by the extension have their behaviour modified; new capabilities are introduced and enforced for all end users. Applications that can be connected to an extended service are provided with the necessary interoperable API which allows integration at the application launching phase.

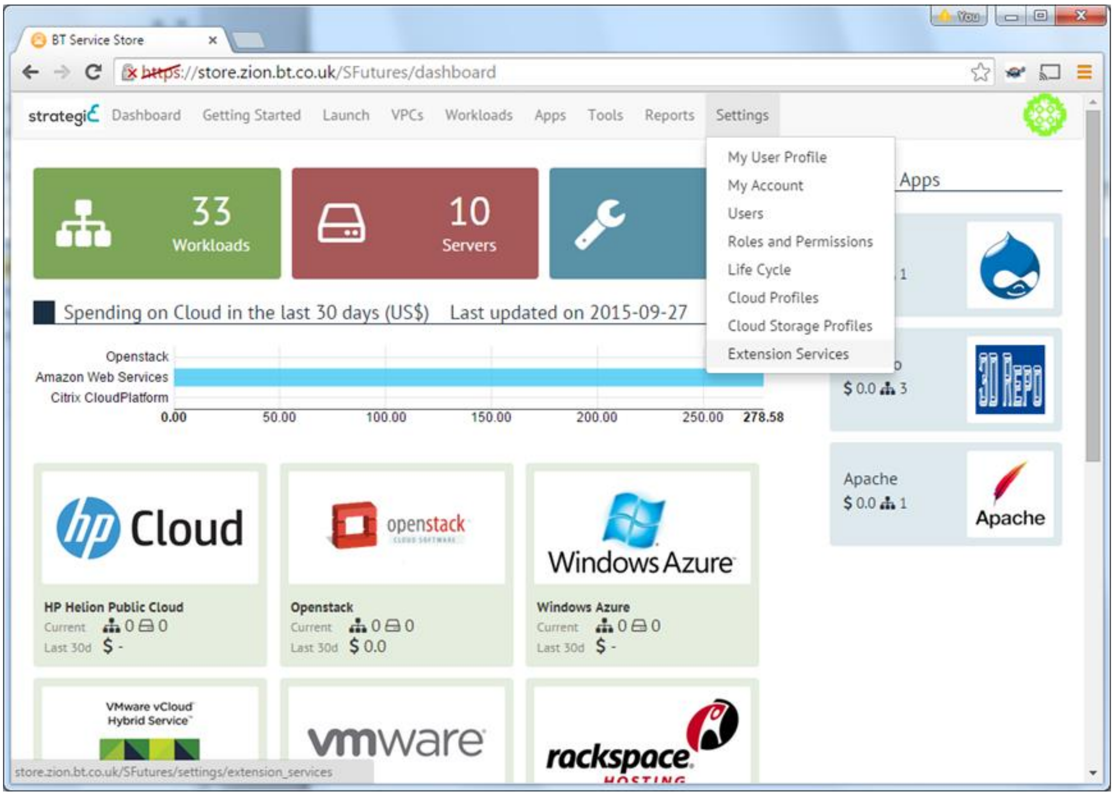
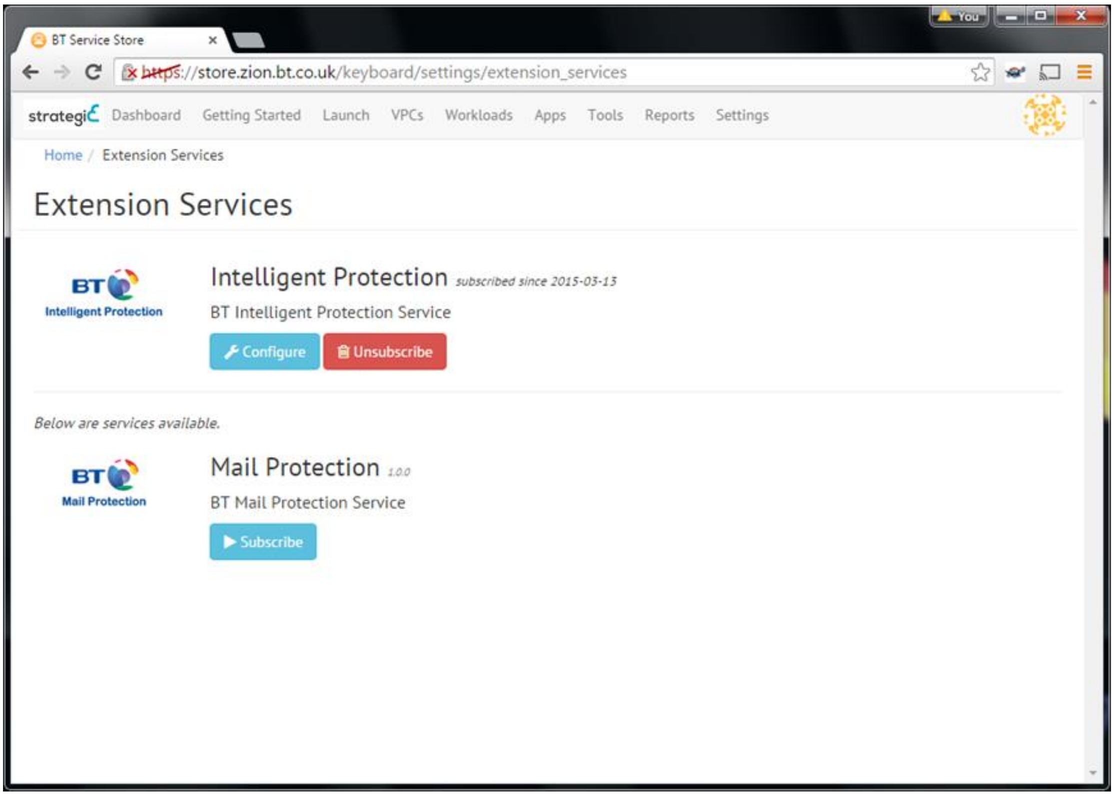


Figure 2: Extension service configuration menu under "Settings"

The user experience for configuring integrated security services via the extension is straightforward. An administrator of a Service Store account needs to navigate to the subscription page (see Figure 2). This will lead to the list of existing extension service page. The services already subscribed to can be configured, otherwise a subscribe button is displayed. The configuration of an extension service leads to a service-specific form.



Extension Services

Intelligent Protection *subscribed since 2015-03-13*

BT Intelligent Protection Service

Below are services available.

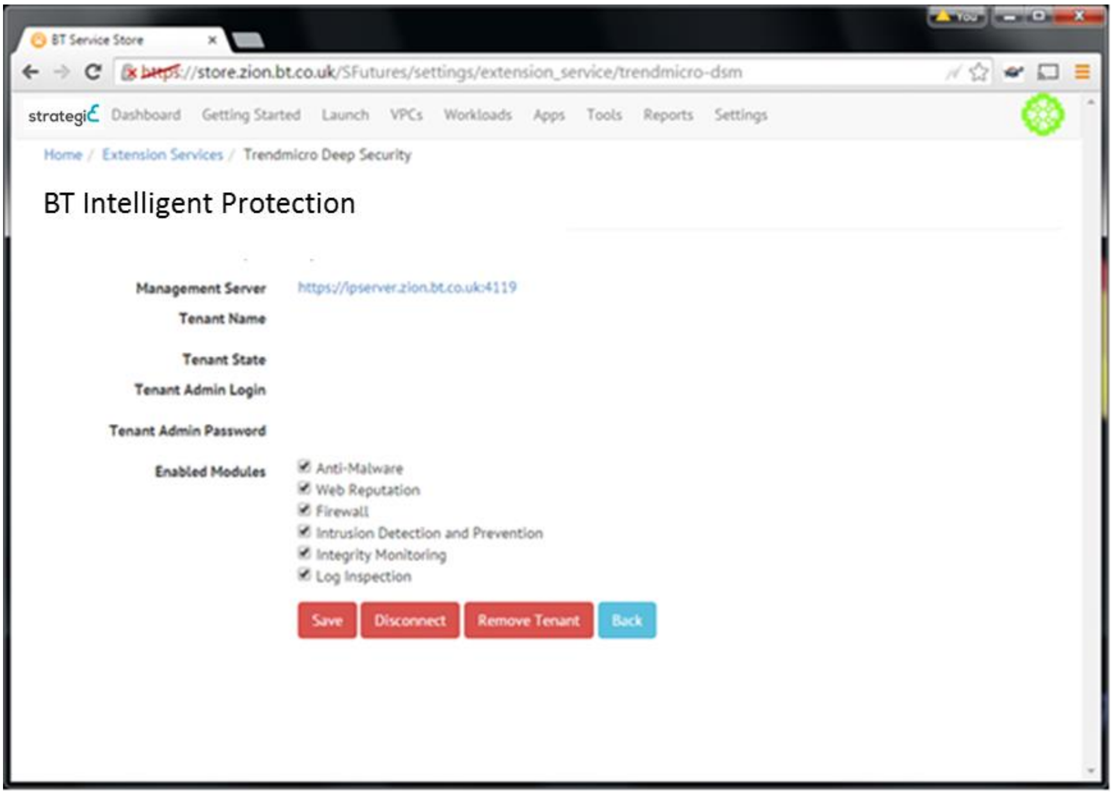
Mail Protection *1.0.0*

BT Mail Protection Service

Figure 3: Available extension services

As an example for the configuration, depicted in Figure 4, Intelligent Protection can either bind into an existing tenant account, or create a new tenant account once this choice has been made, the configuration page displayed The Intelligent Protection is an Application & Host protection service which in the figures we will be replicating with the technology from vendor Trend Micro. The typical configuration is to assign a new tenant for the Service Store account being protected. However, it is also possible to assign an account to an existing tenant, which then merges all the provisioned Infrastructure or services under one dashboard. This would also allow users to apply service extensions across multiple Service Store accounts.

Finally, once an extension service has been subscribed to, the configuration options available will be shown to the user launching a new service. (Launching a new service is achieved by going to the launch icon of the top menu and selecting a service and a cloud target, see deliverable 4.1a [3]). This offers the ability to modify and adapt the extension service to a specific instance either augmenting, or reducing the level of protection. This is illustrated on Figure 5.


BT Service Store
https://store.zion.bt.co.uk/SFutures/settings/extension_service/trendmicro-dsm
strategiC Dashboard Getting Started Launch VPCs Workloads Apps Tools Reports Settings
Home / Extension Services / Trendmicro Deep Security
Save
Disconnect
Remove Tenant
Back

BT Intelligent Protection

Management Server https://ipserver.zion.bt.co.uk:4119

Tenant Name

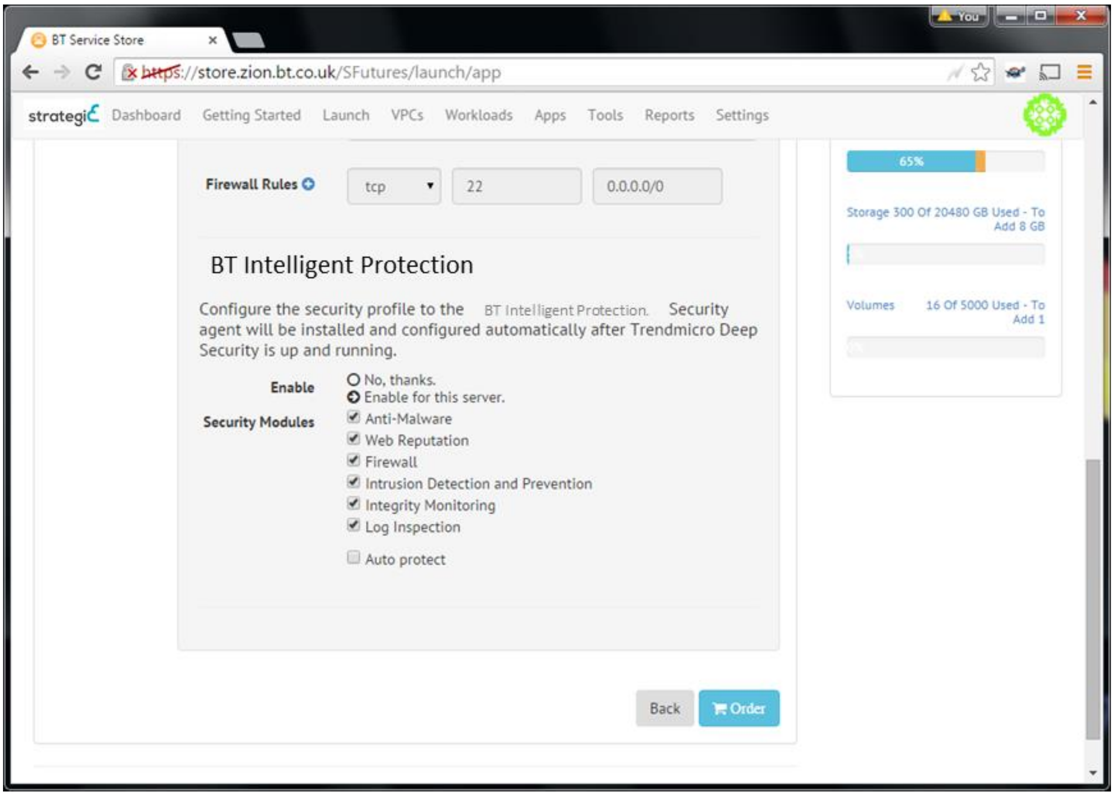
Tenant State

Tenant Admin Login

Tenant Admin Password

Enabled Modules
☑ Anti-Malware
☑ Web Reputation
☑ Firewall
☑ Intrusion Detection and Prevention
☑ Integrity Monitoring
☑ Log Inspection

Figure 4: Configuration of Intelligent Protection


BT Service Store
https://store.zion.bt.co.uk/SFutures/launch/app
strategiC Dashboard Getting Started Launch VPCs Workloads Apps Tools Reports Settings
65%
Back
Order

Firewall Rules tcp 22 0.0.0.0/0

Storage 300 Of 20480 GB Used - To Add 8 GB

Volumes 16 Of 5000 Used - To Add 1

BT Intelligent Protection

Configure the security profile to the BT Intelligent Protection. Security agent will be installed and configured automatically after Trendmicro Deep Security is up and running.

Enable
○ No, thanks.
● Enable for this server.

Security Modules
☑ Anti-Malware
☑ Web Reputation
☑ Firewall
☑ Intrusion Detection and Prevention
☑ Integrity Monitoring
☑ Log Inspection

□ Auto protect

Figure 5: Final stage of launching any application with dedicated protection configuration enabled

It is possible for the account manager to unsubscribe to an extension service (see Figure 3). The de-provisioning has to return unsubscribed services in a working state. Extension services have de-provisioning functions with logical workflows that can disable and de-register services, as well as restoring working workflows in the management console after a decommissioning request.

3 STRATEGIC Service Store Extension: Provider Reputation

3.1 Trust assessor Overview

In the cloud computing paradigm where software, platform and infrastructure are offered as service, the service consumers often have to make decisions to select the most trustworthy provider. One of the key aspects of trust is what we are able to observe while operating in real environments of the resources and infrastructures under evaluation. In order to determine the level of trust for a particular resource or group of resources there is a monitoring tool (see D.4.1a [3]) that is gathering information when virtual resources are used. The gathered data is then used for calculating a trust rank for a particular service provider.

The trust assessor engine implemented in OPTIMIS project [5] allows us to calculate the rank among different providers based on the experience that both have had together and based on the experience that a specific provider has. With the information retrieved from the monitoring system, the framework is able to check what happens to the services and the infrastructure where these cloud services have been deployed. Measurements like memory usage, CPU number, service workload KPIs, VMs number or network information are valuable to get an opinion of how the service is performing in the infrastructure provided by the infrastructure provider.

The trust model developed in OPTIMIS makes use of the weighted sum of four different types of data to calculate trust rank. The four different data types are (a) quality of service parameters measured by monitor components, (b) indicators compliance of and non-compliance requested parameters at deployment type, (c) rankings provided by the users and (d) behaviour of the users with respect to the usability of services, service providers, and infrastructure providers. Each of these data types are provided by four different components, as shown in Figure 6. The trust value function is shown in Figure 6. The assessor integrated in STRATEGIC makes used of the types 'a' and 'b' as data to be exploited to determine the rank for an infrastructure provider.

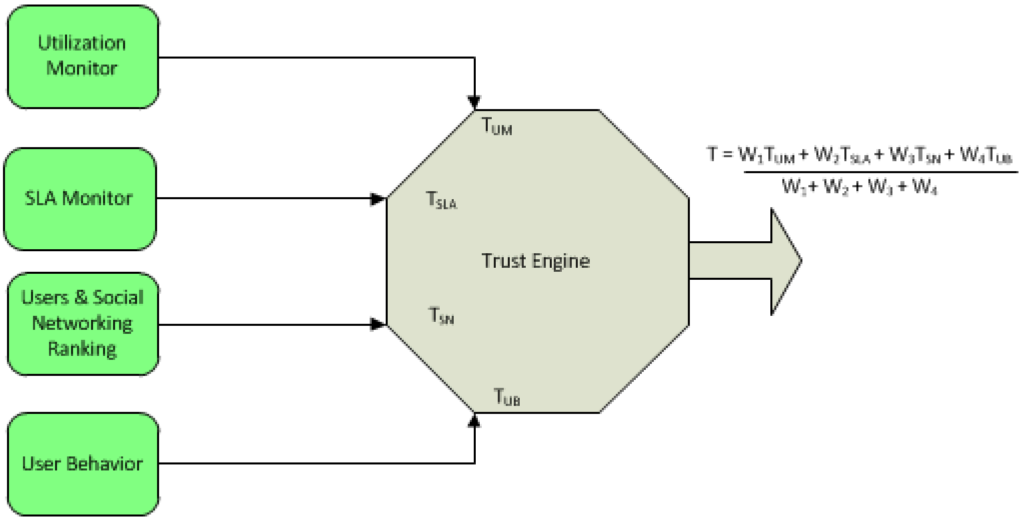

Utilization Monitor
SLA Monitor
Users & Social Networking Ranking
User Behavior
T_{UM}
T_{SLA}
Trust Engine
T_{SN}
T_{UB}
$T = \frac{W_1T_{UM} + W_2T_{SLA} + W_3T_{SN} + W_4T_{UB}}{W_1 + W_2 + W_3 + W_4}$

Figure 6: Trust rank calculation

Figure 6 illustrates how different aspects of the model are used to calculate a comprehensive trust rank. The trust rank used describes different trust levels from the minimum (0) to 5, each level requires minimum values for certain aspects. In the scope of STRATEGIC, the trust model will be populated with the data gathered from the monitoring system running alongside with the STRATEGIC Service Store.

3.1.1 Technical Design and Implementation

The Trust Framework is released under Apache License v2. It is one of the tools developed in the scope of TREC tools in the OPTIMIS research project, the third release of the tool has been included as part of the OPTIMIS Toolkit package released at the end of the research project.

The component is released as a WAR file previously deployed and tested over Tomcat 6.X and 7. The component can be used by invoking the APIs through HTTP calls or using the Java client provided importing it as a library in new projects. The trust assessor can act as an autonomy services, the component provides a REST API, which other services can access.

The framework is split into four (4) different logic sections based on the capabilities and functionalities they provide:

- TrustFrameworkService/IPTrustFramework: This module contains the main logic of the component to calculate trust for infrastructure providers.
- TrustFrameworkDB/iptrustdb: Data access objects for performing operations in the database.
- TrustFrameworkDB/sptrustdb: Data access objects for performing operations in the database.
- TrustFrameworkClients: Client that accesses programmatically to the REST APIs provided.

We aim at determining whether infrastructure providers are allocating and managing resources in the requested way. In order to meet this goal, STRATEGIC performs various integration activities in order to support the reputation functionality offered by the assessor. The tool released by OPTIMIS was developed using Nagios monitoring system for the monitoring of physical resources as well as used several collector scripts in charge of monitoring of virtual resources via libvirt. In order to incorporate the component functionality into STRATEGIC we had to decouple the original component from the default monitoring systems and develop appropriate links to our STRATEGIC monitoring tools based on Zabbix. In addition, the SLA manager component is not present in the STRATEGIC platform as it was in OPTIMIS, STRATEGIC does not provide access to the platform programmatically to monitor the agreement terms. The reputation component used in STRATEGIC gathers information from the monitored resources according to resources defined by the deployment request.

Figure 7 and Figure 8 depicts the different subsystems used to obtain the reputation.

More specifically, Figure 7: Trust Framework high-level architecture shows at high level how the reputation engine interacts with the monitoring system in charge of the population of the models used within the trust framework. The framework is accessible through REST API (some data is also exposed via web interface) and uses a MySQL database to store intermediate results.

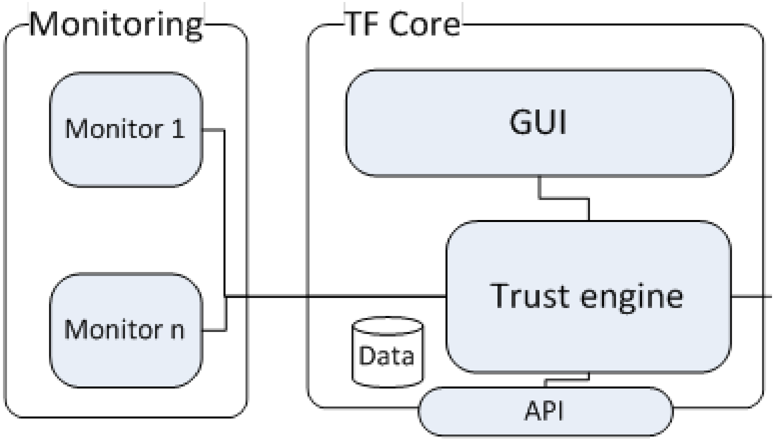


Figure 7: Trust Framework high-level architecture

On the other hand, Figure 8: Monitoring system low **level** gives a low level overview of the components that compose the monitoring process and as well as how the remote monitoring agents gather the measurements. Further information on the monitoring system and its integration with the Service Store can be found in D.4.1.a [3].

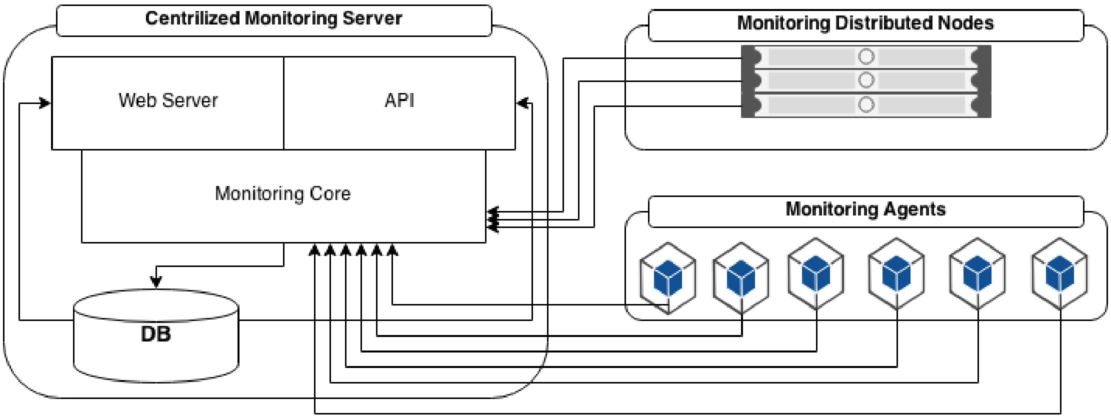


Figure 8: Monitoring system low level

Figure 9 illustrates the class diagram of the software tool used to provide the final reputation rank; the TrustManager is the core entity in charge of the calculation of the trust rank. The component has a database associated to store intermediate results needed for the calculation. The software tool also offers social networking capabilities that allow sharing information with other infrastructure providers; however, STRATEGIC does not incorporates this functionality.

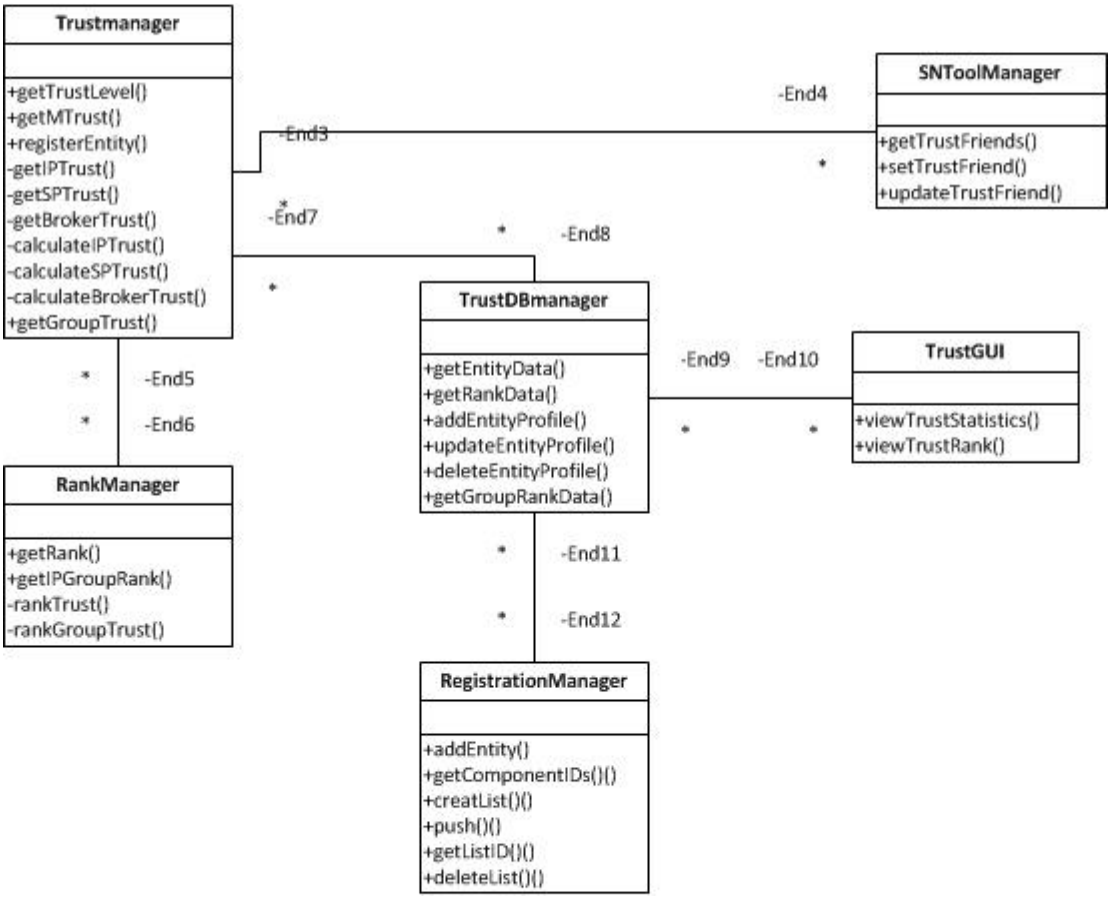


Figure 9: Reputation system class diagram

While the interactions with the monitoring system have been validated, the reputation algorithms need to be populated with data coming from pilot operations to assess the component functionality (D.4.1c). The Trust Assessor performed forecast based on previous measurements, it is necessary to have enough data because of the algorithm used (Holt-Winters) in order to avoid inaccurate results, even if with 48 hours data is enough, it has been proved that calculations with at least two weeks of data obtains better results. The component was tested against a monitoring system following the specifications described in D.4.1a [3]. Every virtual machine deployed is mapped in the monitoring system using the monitoring path convention (OrganizationName::Workload_Identifier::Image_Identifier).

4 Conclusions

The second iteration of the STRATEGIC Cloud Broker offers to the pilot partners the ability to deploy their cloud based applications, from a centralized dashboard provided by the Service Store, together with the security services.

These services were integrated as extension services and are presented as subscription based consumables. BT Intelligent Protection service has already been on boarded using this framework to cover the application & host protection requirements. The user journey has also been summarised in section 2.3. The integration of data encryption as a service is underway using the same framework and the details for which will be published in the final iteration of this deliverable.

The document also provides an overview of the integration of the infrastructure provider reputation mechanisms, which we are able to populate interacting with the monitoring services associated with the STRATEGIC Service Store.

This deliverable, together with the first iteration, provides a description of the design and architecture of the marketplace. This description supports the pilot partners to operate their applications benefiting from the horizontal security services.

5 References

[1] STRATEGIC Deliverable 2.3, Framework Architecture and Technical Specification

[2] STRATEGIC Deliverable 3.1, Specification of Cloud-Enablement and Migration Solutions and Services. Public report.

[3] STRATEGIC Deliverable D.4.1.a STRATEGIC Cloud Broker / Marketplace. Public report.

[4] STRATEGIC Deliverable 5.1a, Cloud Enablement of Distributed Services. Public report.

[5] OPTIMIS Toolkit. (http://optimistoolkit.com/)