COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME

CIP-ICT-PSP-2013-7

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

Deliverable D4.2b

Migration, Adaptation, Localization and Governance Tools

Workpackage	WP4 – Framework Implementation, Integration and Test
Editor(s):	Giannis Ledakis, Panagiotis Gouvas, Juri Hudolejev, Ilja Livenson
Responsible Partner:	SingularLogic Information Systems & Applications SA, National Institute of Chemical Physics and Biophysics
Quality Reviewers	Fotis Karayannis (URNS), Géry Ducatel (BT), Joshua Daniel (BT), Christos Kanellopoulos (URNS)
Status-Version:	v1.0
Date:	03/08/2015
EC Distribution:	Public
Abstract:	This deliverable reflects the outcomes of tasks T4.1 and T4.3 covering design and description of the migration, adaptation, localization and governance services of the STRATEGIC platform.

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	13/10/2014	Draft Table of Contents (ToC)	NICPB
v0.2	19/11/2014	Extended cloud enablement section, ToC updates from SiLO	NICPB, SiLO
V0.3	6/07/2015	Gap analysis outcome, analysis method	NICPB
V0.4	17/07/2015	Integrated input from SILO, extension of the document	SILO, NICPB
V0.5	22/07/2015	Changes based on initial feedback from URNS and ATOS	SILO
V0.6	23/07/2015	Integrated version	NICPB
V0.7	27/07/2015	Partially addressed comments from URNS	NICPB
V0.8	29/07/2015	Integrated version, addressed all URNS comments	SILO
V0.9	30/07/2015	Integrated version, addressed all BT coments	SILO
V1.0	1/08/2015	Final polishing, comments from URNS	NICPB

Table of Contents

List of Figures

List of Tables

Definitions, Acronyms and Abbreviations

Acronym	Title
API	Application Programming Interface
BT	British Telecommunications
CKAN	Comprehensive Kerbal Archive Network
IaaS	Infrastructure as a Service
ISV	Independent Software Vendor
IP	Infrastructure Provider
OS	Operating System
REST	Representational State Transfer
UI	User Interface
URL	Uniform Resource Locator
VPN	Virtual Private Network

Table 1: Definitions, Acronyms and Abbreviations

Executive Summary

The target of this deliverable is to describe the application migration, adaptation, localization and governance tools offered through the STRATEGIC Service Store. The work is based on the specification defined in D3.2 and is complementary to that document.

This is a second iteration of the deliverable and should be seen as a complimentary to the first one released in M12 – D4.2a. The content of this deliverable is based on the gap analysis of the functionality offered by the STRATEGIC platform including features that were exposed since the D4.2a delivery, as well as feedback from migrating pilot applications to STRATEGIC platform in WP5.

The second version of the deliverable extends on the following aspects:

- Descriptions of role-based user flows based on gap analysis and experience from the activities in WP5. Analysis outcome was summarised in a matrix.
- Providing a public sector administrator’s guide regarding inclusion of a regional IaaS – an important aspect for cloudification of data-sensitive pilot use cases.
- Description of localization of deployments to allow respecting of public sector requirements towards data preservation and legal aspects.
- Governance process is extended to cover also STRATEGIC Service Store related account management that allows delegating service governance within a particular public sector organization.
- Linking of security related aspects to the migration, adaptation, localization and governance aspects of STRATEGIC platform. Please note that the in-detail descriptions of the security components are done in the corresponding deliverables. This one serves as integration point only. In particular, integration with STORK and SEMIRAMIS was positioned, as well as BT Intelligent Protection and Intelligent Data Protection services.

This deliverable concludes tasks T4.1 and T4.3 and serves along with D4.2a as input regarding tools for migration and operation of STRATEGIC applications in WP5.

1 Introduction

1.1 Scope and purpose of the document

The main goal of the STRATEGIC project is to facilitate organisations and notably public bodies to leverage the benefits of public cloud services, through boosting three complementary adoption directions: (a) the porting of existing on-line services to the Cloud, (b) the adaptation and localisation of existing services, which have been successfully deployed by other organisations and (c) the composition of new public cloud services on the basis of available legacy services.

This deliverable is the second part of D4.2 and serves as outcome of the task T4.1. The focus of the task was on the provision of a range of tools that would enable cloud developers and ISVs to migrate distributed services to the cloud and adapt and localize them on deployment. In addition, methods for integration with multiple IaaS systems were to be analysed.

Current deliverable concentrates on extensions and filling in the gaps of the tools for migration, adaptation, localization and governance.

The task was relying on the brokerage services and the STRATEGIC Service Store developed in Task 4.2.

The purpose of the document is description of the devised tools and processes for the goals of the task 4.1.

1.2 Target audiences

The target audience for this document is the technical partners of this project, the technical administrators of the Pilots and the independent software vendors (ISV) who wish to resell applications through the STRATEGIC Service Store.

1.3 Structure of the document

This document is split into four main chapters in addition to Chapter 1 and they comprise of:

- The Chapter 2, "Tools usage matrix", presents gap analysis performed for the role-based tools usage;
- The following Chapters are providing inputs for filling in the identified gaps.
- The last chapter is Conclusion of the document.

2 Tools usage matrix

In order to verify that all of the possible scenarios have been covered, a gap analysis was performed against the updated planned roles and features of the STRATEGIC platform. The gap analysis was used to drive creation of the content for this deliverable.

At the moment of writing, the following user roles are identified for the STRATEGIC platform:

- ISV / Integrator – a technical party providing application packaging services for the public sector clients or promoting their own packaged solutions through the marketplace.
- IaaS Operator – a role responsible for operating an IaaS solution that can be integrated with a common STRATEGIC service store.
- Service Store operator – a role responsible for operating the marketplace granting access to other roles as well as publishing packaged solutions to all of the public sector users.
- Public sector administrator – a role responsible for maintaining technical infrastructure of the public sector client.

The usage matrix for these roles and the functionality offered by STRATEGIC platform is given below. The cells of the matrix correspond to the description of the flows for a particular role and aspect. "N/A" means that the flow doesn't make sense due to a missing business need. "D4.2a" means that the flow is covered in the corresponding deliverable. "Missing/partial" means that the flow description is not present and should be covered or extended in this deliverable.

	ISV / Integrator	**IaaS Operator**	**Service Store operator**	**Public sector administrator**
Cloud-enablement	D4.2a	N/A	N/A	N/A
Infrastructure on-boarding	N/A	D4.2a	D4.2a	**missing**
Application migration between IaaS	N/A	N/A	N/A	D4.2a
Application adaptation	D4.2a, **partial**	N/A	N/A	N/A
Application localisation	N/A	N/A	N/A	D4.2a
Application governance	N/A	N/A	**missing**	D4.2a
STORK & SEMIRAMIS Integration	**missing**	N/A	N/A	N/A
Application and host protection	**missing**	**missing**	**missing**	**missing**
Data protection and encryption as a service	**missing**	**missing**	**missing**	**missing**

Table 2: Gap analysis table for the role-based flows

In addition, another role - **Managed security provider** – was identified, specific to the Application and host protection as well as Data protection and encryption services. The role is responsible for providing security policies for the client environments.

The rest of the document is dedicated to covering the gaps that came from this matrix. Each cell that is identified as requiring additional input is expanded and grouped under a particular topic. If another deliverable is concentrating on a particular aspect, only a high level overview is provided in this document along with a reference to a concrete deliverable.

3 Infrastructure on-boarding

Infrastructure on-boarding means making a specific cloud available to STRATEGIC Service Store. As described in deliverable D4.2a [1], infrastructure on-boarding is a task that is mainly addressed by IaaS and Service Store Operators. However, public sector administrators have to enable the use of the particular cloud and register it under his Service Store account. This procedure is described in the following section 3.1.

3.1 Infrastructure on-boarding for public sector administrator

A public sector administrator has to enable the use of the particular cloud and register it under his Service Store account. In order to achieve this, a public sector administrator should use both the IaaS dashboard and STRAGEGIC Service Store. This specific procedure can be also described as infrastructure instantiation, and the steps needed in both IaaS dashboard and STRATEGIC Service Store are described in this section.

In order to allow public sector administrator to deploy services for the end-users, the IaaS must become available to STRATEGIC Service Store. This process includes network configuration by IaaS operators in order to allow connections between the IaaS and configuration from Service Store administrator, as described in deliverable D4.2a [1].

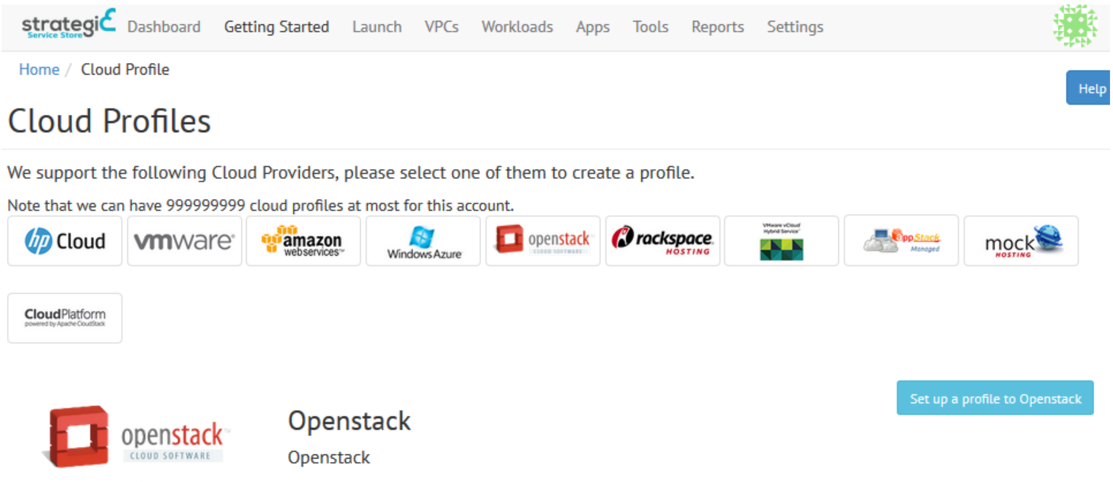
After this process takes place, public sector administrator can use STRATEGIC Service Store Cloud Profile Management to provide the credentials needed from STRATEGIC Service Store for accessing IaaS APIs. This means that public sector administrator must have an appropriate account on an IaaS that has been imported to STRATEGIC Service Store. STRATEGIC Service Store supports the following platforms:

- Rackspace[1]
- VMWare VCloud[2]
- Amazon AWS account[3]
- HP Cloud[4]
- Windows Azure[5]
- CloudPlatform[6]
- OpenStack[7]
- BT Cloud[8]

[1] http://www.rackspace.com/
[2] http://www.vmware.com/products/vcloud-suite
[3] http://aws.amazon.com/
[4] http://www.hpcloud.com/
[5] http://azure.microsoft.com/
[6] http://www.citrix.com/products/cloudplatform/overview.html
[7] http://www.openstack.org/
[8] https://btcloud.bt.com/

As OpenStack is the IaaS platform used by the pilot scenarios of two pilots in STRATEGIC, further instructions are concentrating on that platform. However, this process is very similar for every Cloud platform used.

After logging to STRATEGIC Service Store, public sector administrator has to create a cloud profile. First step needed is the selection of appropriate cloud provider like Amazon Web Services or platform like OpenStack.



Cloud Profiles

We support the following Cloud Providers, please select one of them to create a profile.

Note that we can have 999999999 cloud profiles at most for this account.

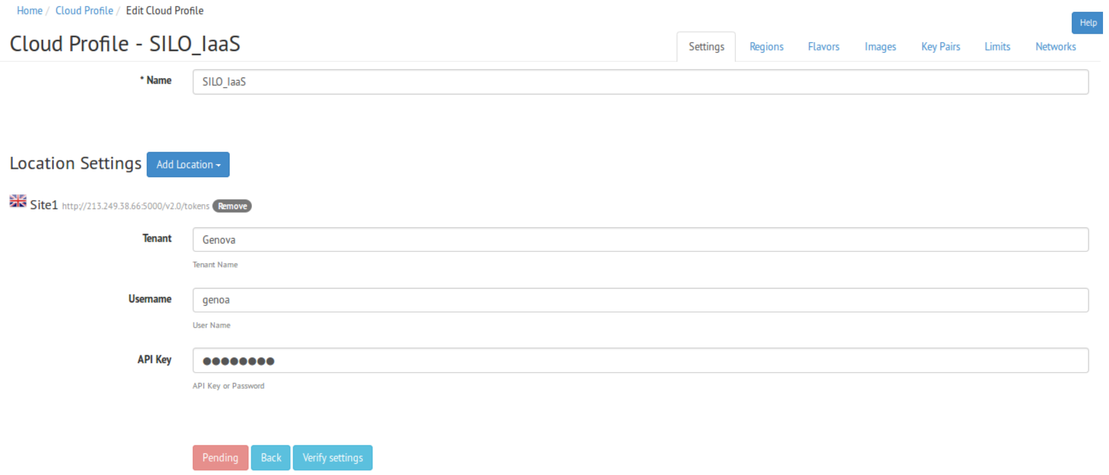
Set up a profile to Openstack

Openstack

Openstack

Figure 1: Selection of a cloud provider for creation of a cloud profile.

After selecting the desired cloud platform, public sector administrator has to provide cloud profile information. For OpenStack cloud profiles, administrator has to provide tenant, username and password information as shown in **Figure 2** below. All this information is available to public sector administrator, as far as he is able to login to the OpenStack IaaS that has been onboarded.



Cloud Profile - SILO_IaaS

* Name: SILO_IaaS

Location Settings

Site1 http://213.249.38.66:5000/v2.0/tokens

Tenant: Genova
Tenant Name

Username: genoa
User Name

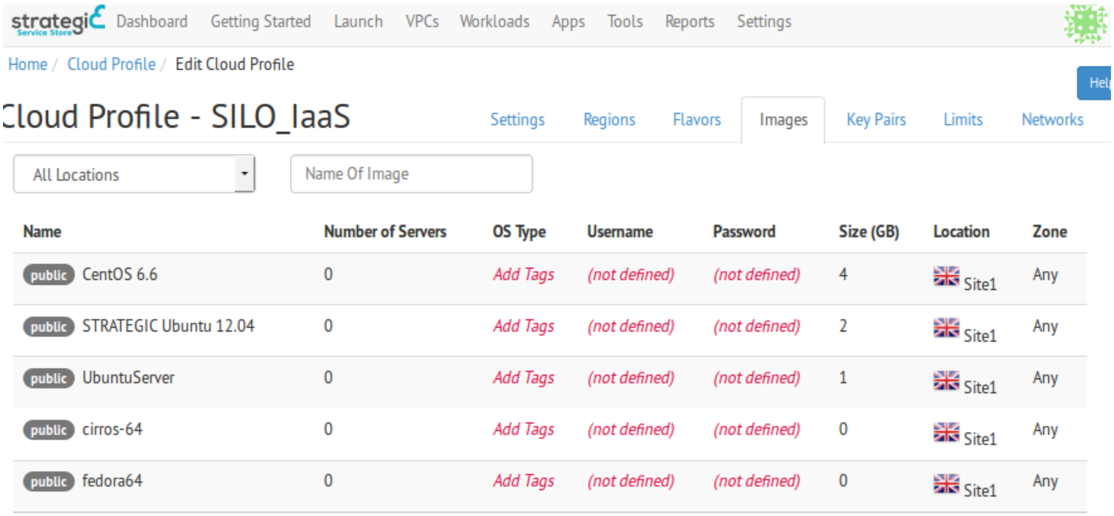
API Key: ●●●●●●●●
API Key or Password

Figure 2: Configuration of a Service Store cloud profile.

By pressing the "*Verify Settings*" button, the credentials are checked for their validity and afterwards can be saved and the cloud profile is available for use.

All the settings that the public sector administrator has created in the IaaS environment should be available for use on the STRATEGIC Service Store. These settings are provided along with IaaS information, templates of virtual hardware available to Virtual Machines (usually called flavors), available Images and Key Pairs.

The Service Store can use the images that are available in the IaaS, as appropriate API calls that fetch image metadata are used. Once images metadata has been fetched it is possible to review and adjust the settings of the images, such as the username and password of the user used to manually connect to the virtual machine, as depicted in **Figure 3**. These images are now available to be used during the deployment phase of services through STRATEGIC Service Store.

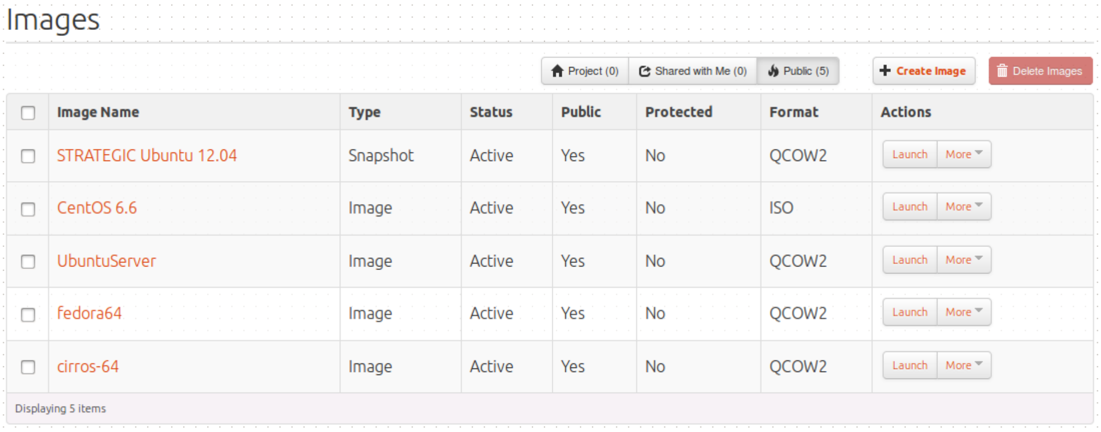


Cloud Profile - SILO_IaaS

Name	Number of Servers	OS Type	Username	Password	Size (GB)	Location	Zone
public CentOS 6.6	0	Add Tags	(not defined)	(not defined)	4	Site1	Any
public STRATEGIC Ubuntu 12.04	0	Add Tags	(not defined)	(not defined)	2	Site1	Any
public UbuntuServer	0	Add Tags	(not defined)	(not defined)	1	Site1	Any
public cirros-64	0	Add Tags	(not defined)	(not defined)	0	Site1	Any
public fedora64	0	Add Tags	(not defined)	(not defined)	0	Site1	Any

Figure 3: Overview of the images available in a particular IaaS through STRATEGIC Service Store.

Most IaaS are allowing the usage of custom Operating System(OS) images, so it is important that the OS images provided by the IaaS can support the needs of public sector administrators, for example the need of specific OS, specific OS version or even images of an OS snapshot. An example listing of OS images as displayed in the OpenStack UI is provided in the following figure.

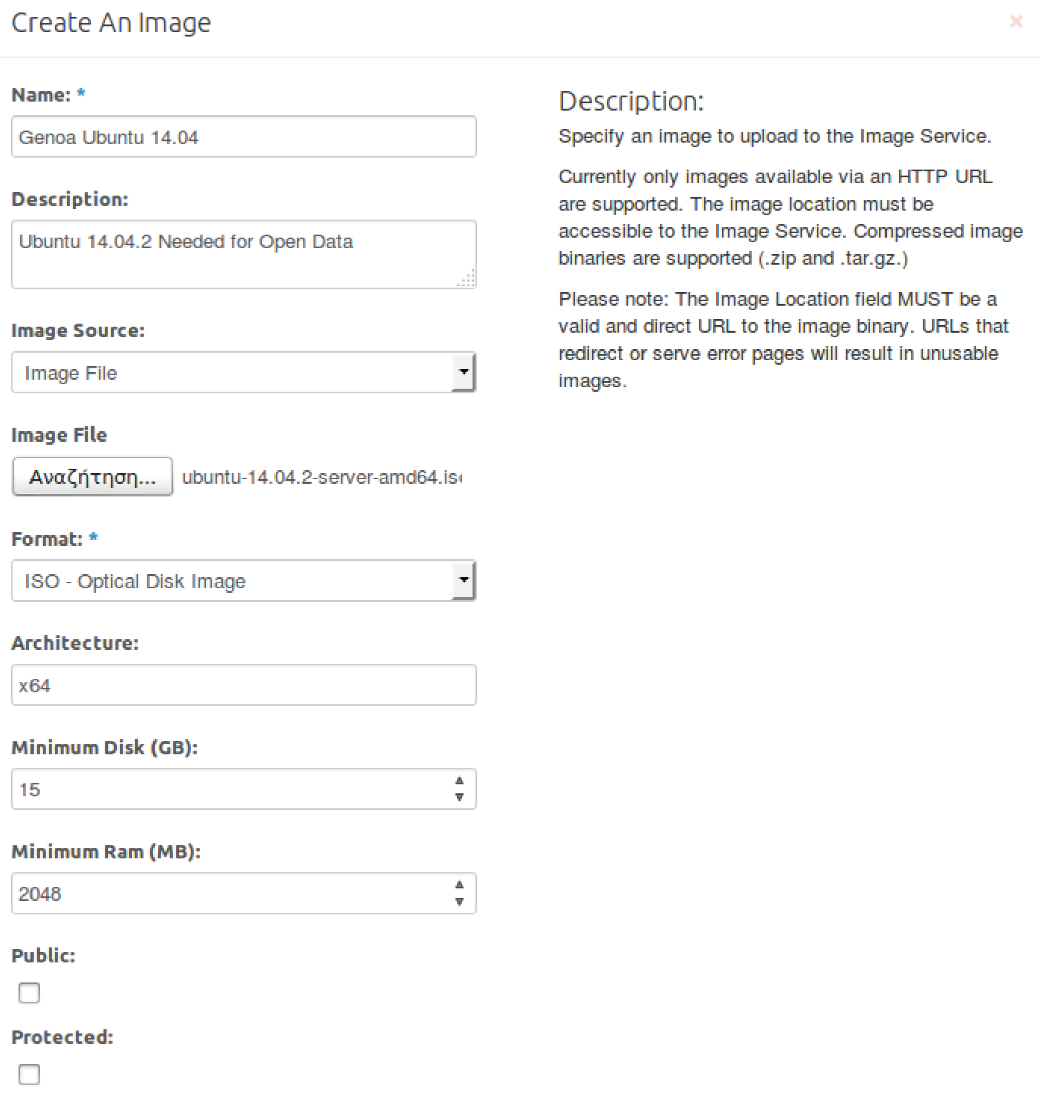


☐	Image Name	Type	Status	Public	Protected	Format	Actions
☐	STRATEGIC Ubuntu 12.04	Snapshot	Active	Yes	No	QCOW2	Launch More
☐	CentOS 6.6	Image	Active	Yes	No	ISO	Launch More
☐	UbuntuServer	Image	Active	Yes	No	QCOW2	Launch More
☐	fedora64	Image	Active	Yes	No	QCOW2	Launch More
☐	cirros-64	Image	Active	Yes	No	QCOW2	Launch More

Displaying 5 items

Figure 4: Listing of the OS images in a particular OpenStack deployment.

New images cannot be added through STRATEGIC Service Store but only though the specific IaaS. With the precondition that permissions of IaaS allow it, public sector administrator can upload the appropriate OS images to be used. A sample of this process is presented in **Figure 5** that follows.



Create An Image

Name: *

Genoa Ubuntu 14.04

Description:

Ubuntu 14.04.2 Needed for Open Data

Image Source:

Image File

Image File

ubuntu-14.04.2-server-amd64.is

Format: *

ISO - Optical Disk Image

Architecture:

x64

Minimum Disk (GB):

15

Minimum Ram (MB):

2048

Public:

□

Protected:

□

Description:

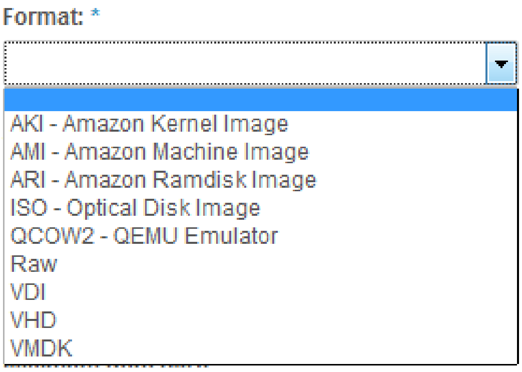
Specify an image to upload to the Image Service.

Currently only images available via an HTTP URL are supported. The image location must be accessible to the Image Service. Compressed image binaries are supported (.zip and .tar.gz.)

Please note: The Image Location field MUST be a valid and direct URL to the image binary. URLs that redirect or serve error pages will result in unusable images.

Figure 5: Creation of a new OS image.

Images on OpenStack can be uploaded from local disk or even fetched directly from http URL if the image location is directly accessible to the Image Service of OpenStack. Images of various formats can be used, either directly or in compressed image binaries of .zip and .tar.gz format. Supported image types are depicted in **Figure 6**.



Format: *

AKI - Amazon Kernel Image
AMI - Amazon Machine Image
ARI - Amazon Ramdisk Image
ISO - Optical Disk Image
QCOW2 - QEMU Emulator
Raw
VDI
VHD
VMDK

Figure 6: Supported image types.

The images to be provided to OpenStack or any other cloud platform should be specific images prepared for usage on cloud environments. Images of popular OS are usually distributed in cloud specific versions, like the Cloud versions of Ubuntu[9]. These can be directly provided to OpenStack, CloudStack or any other STRATEGIC Service Store compliant IaaS and then used from public sector administrators.

Even if there is a specific OS that is not provided as Cloud image, it can be prepared by executing the following methodology for creating VM snapshots as templates for usage on Cloud. Although some differences might exist between different IaaS providers and the different OS, the main path is the same.

1) Import OS image to the IaaS by using appropriate IaaS menus
2) Launch a VM with the selected OS image
3) Install OS on the launched VM
4) Install XenServer tool[10] in the installed OS(in order to enable Xen hypervisor. Other hypervisors can also be enable by installing corresponing tools)
5) Install and configure cloud-Init to handle the early initialization of cloud instances(Other tools can also be used but cloud-init is considered a defacto choice[11] and used existing cloud images[12])
6) Build Template Image based on the running VM and add corresponding tags
7) Synchronize STRATEGIC Service Store to retrieve the newly added image

For security reasons, it also highly suggested to delete the default accounts and cleanup (of history, path, network specific information) before the build of any template image.

Information with details about the specific procedure needed is usually provided by the IaaS platform used. For example, on OpenStack concrete examples exist in the OpenStack documentation[13]. Also, samples of the methodology of creating OS templates based on snapshots is provided in APPENDIX A: Preparing VM template based on Ubuntu 12.04LTS / 14.04LTS and APPENDIX B: Preparing VM template based on CentOS.

This methodology also allows the creation of VM templates with preconfigured services, thus enabling the easy deployment of existing services. This way VMs have been created that have preconfigured services needed to support the Stork and Semiramis scenarios of STRATEGIC.

The municipality administrator can also see an overview or specific details like flavours (depicted in Figure 7), network, and possible limitations of the IaaS in separate tabs, thus validating the proper instantiation of cloud profile in STRATEGIC Service Store.

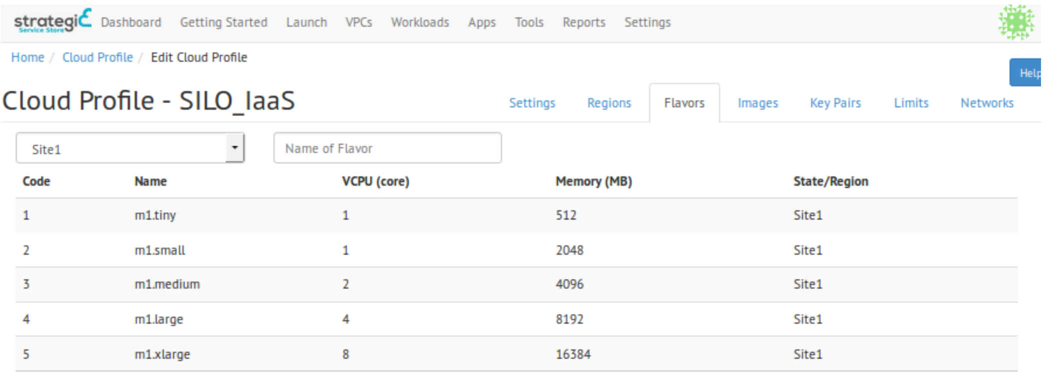
[9] https://cloud-images.ubuntu.com/

[10] http://xenserver.org/open-source-virtualization-download.html

[11] https://cloudinit.readthedocs.org/en/latest/

[12] https://help.ubuntu.com/community/CloudInit

[13] http://docs.openstack.org/image-guide/content/ubuntu-image.html



Home / Cloud Profile / Edit Cloud Profile

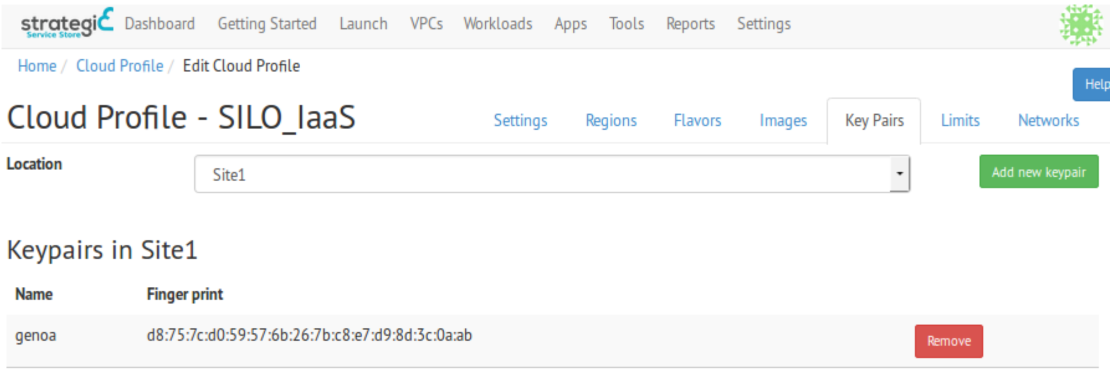
Cloud Profile - SILO_IaaS

Site1 | Name of Flavor

Code	Name	VCPU (core)	Memory (MB)	State/Region
1	m1.tiny	1	512	Site1
2	m1.small	1	2048	Site1
3	m1.medium	2	4096	Site1
4	m1.large	4	8192	Site1
5	m1.xlarge	8	16384	Site1

Figure 7: Overview of the configured hardware flavours.

An important factor that public sector administrator has to set up before being able to deploy a service through STRATEGIC Service Store is the Key Pairs. Key Pairs are used to allow STRATEGIC Service Store to connect to the instantiated virtual machine and manage them in automated way in order to install the needed applications and deploy the services. Key Pairs can be created directly in IaaS as presented in **Figure 8** if this is supported from IaaS API.



Home / Cloud Profile / Edit Cloud Profile

Cloud Profile - SILO_IaaS

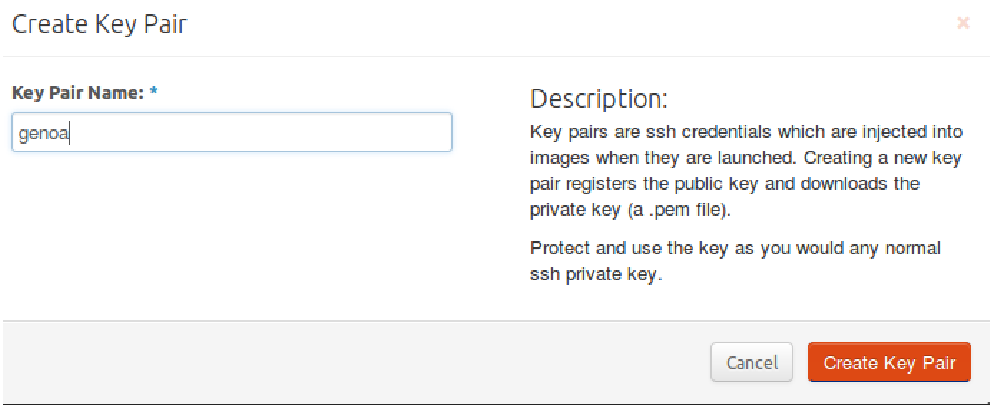
Location: Site1

Keypairs in Site1

Name	Finger print
genoa	d8:75:7c:d0:59:57:6b:26:7b:c8:e7:d9:8d:3c:0a:ab

Figure 8: Key management in STRATEGIC Service Store. Keys will be used for system level access to the provisioned VMs.

If this process in not supported, the administrator has to access IaaS UI and register and create appropriate private/public key pairs like in **Figure 9.** However, there is no need to download the specific key pair created, as it will be automatically fetched by the Service Store.



Create Key Pair

Key Pair Name: * genoa

Description:

Key pairs are ssh credentials which are injected into images when they are launched. Creating a new key pair registers the public key and downloads the private key (a .pem file).

Protect and use the key as you would any normal ssh private key.

Figure 9: Initiate key creation in OpenStack IaaS.

4 Migration

Application migration is a process of moving application from one IaaS provider to another. Although STRATEGIC Service Store supports the adaptation and deployment of published services, sometimes might be needed to fully migrate an existing server. The migration process on STRATEGIC can be related of the server that hosts a public service, at VM level. The specific methodology supported by STRATEGIC Service Store is called Binary Image Re-contextualisation and has been fully covered in D4.2a, thus no further extensions were found needed in this deliverable.

5 Adaptation and localization tools

One of the core features that STRATEGIC framework is offering is the ability to adapt and localize existing public services. STRATEGIC Service Store offers tools that allow making application adaptable to particular deployments. A complimentary set of tools is aimed at providing localisation capabilities by allowing setting configuration parameters during provisioning that both restrict and configure application to comply with user requirements.

5.1 Adaptation by ISV/Integrator

One of the most important aspects offered by the STRATEGIC Service Store is the ability to adapt published applications. Adaptation means exposure of certain parameters of the application that can the end user can modify. For example, for OpenData CKAN platform, it could be a site name and a set of plugins that should be enabled. This allows applications to be deployed multiple times and configured based on specific needs and also to be re used by other actors, including other municipalities' administrators.

The specific procedure needed to be done by ISVs or Integrators (depending on the ownership model) in order to make and application adaptable through STRATEGIC Service Store has been already described in deliverable D4.2a [1], a procedure of specifying the metadata of STRATEGIC Workload Metadata Model that are describing the application and has been documented in deliverable D3.1 [2]. In deliverable D4.2a [1] the provided interface and capabilities that can be used by public sector administrator during or even after the deployment process has been described.

Adaptation of a deployed application is not possible for security reasons by the Service Store administrator, who is only related to the process of validating applications to be the STRATEGIC Service Store before they are being published.

5.2 Localization

Localization of existing public services refers to the solutions and tools that allow the adaptation of the application for specific needs based on local and international requirements shaped by legal constraints related to security and privacy. STRATEGIC can serve the localization needs by a combination of different aspects provided.

One aspect of localization is addressed by the adaptation capabilities that allow public bodies from different countries to configure application according to specific needs, like translation of basic application text fields, for example, application title, header, or adapting parameters to support local restrictions, for example, configuring application for connection to VPN.

STRATEGIC Service Store however can provide localization support on higher level. By integrating parts of OPTIMIS toolkit[14] to extend the descriptive capabilities of the STRATEGIC Workload Metadata Model, with country specific information, the Service Store gains the ability to filter the target providers to guarantee that the infrastructures provided to public bodies compiles with their

[14] http://optimistoolkit.com/

legal constraints and their key data protection considerations. The STRATEGIC Workload Metadata Model tries to model and describe the semantics of any possible workload. But in order to describe the constraints and restrictions that public bodies have in order to take into consideration their data protection requirements as well as their localization needs, Optimis Service Manifest[15] is used.

Optimis Service Manifest consists of many different elements; however, DataProtectionSection describes the localization part that we want in STRATEGIC. DataProtectionSection basic internal element is EligibleCountryList that records the countries that an application is eligible for deployment. At the same time a supplementary list of the non-eligible countries can be provided in the NonEligibleCountryList, if the purpose of localization filtering is to only block specific countries. Required data protection (DataProtectionLevel) and data encryption (DataEncryptionLevel) levels can also be defined along with the localization requirements, thus helping ensure that legal constrains are easier met. The data protection requirements defined in Optimis Service Manifest are also presented in Table 3.

```
<xs:simpleType name="DataProtectionLevelType">

<xs:restriction base="xs:string">

<xs:enumeration value="DPA"/>

<xs:enumeration value="None"/>

</xs:restriction>

</xs:simpleType>

[…]

<xs:complexType name="EncryptionLevelType">

<xs:choice>

<xs:sequence>

<xs:element name="EncryptionAlgoritm" type="opt:EncryptionAlgoritmType"/>

<xs:element name="EncryptionKeySize" type="xs:int" default="128"
minOccurs="0"/>

</xs:sequence>

<xs:sequence>

<xs:element name="CustomEncryptionLevel" type="xs:anyType"/>

</xs:sequence>

</xs:choice>
```

[15] https://packcs-e0.scai.fraunhofer.de/service-manifest-snapshot/

```
</xs:complexType>
```

Table 3: Part of data protection requirements as defined in Optimis (source: Optimis D7.2.1.3 Cloud Legal Guidelines [3])

An example of the elements defined in the schema is presented in Table 4.

```
<opt:DataProtectionSection>

<opt:EligibleCountryList>

<opt:Country>DE</opt:Country>

</opt:EligibleCountryList>

<opt:NonEligibleCountryList>

<opt:Country>AF</opt:Country>

</opt:NonEligibleCountryList>

<opt:DataProtectionLevel>DPA</opt:DataProtectionLevel>

<opt:DataEncryptionLevel>

<opt:EncryptionAlgoritm>AES</opt:EncryptionAlgoritm>

</opt:DataEncryptionLevel>

<opt:DataStorage>

<opt:AllocationUnit>byte * 2^20</opt:AllocationUnit>

<opt:Capacity>500</opt:Capacity>

</opt:DataStorage>

</opt:DataProtectionSection>
```

Table 4: Example of localization information stored in Optimis (source: Optimis D7.2.1.3 Cloud Legal Guidelines [3])

Optimis can use the defined requirements of Optimis Service Manifest in order to filter suitable infrastructure providers based on compliance of providers' regional information with pilot and application needs. This capability of Optimis addresses the localization needs of STRATEGIC Service Store.

Two approaches were considered for the integration of STRATEGIC Service Store with Optimis; First approach considered is the extension of STRATEGIC Workload Metadata Model with the parts of Optimis Service Manifest. Although the extension on metadata level would be easy, there would be also the need to create the mechanisms that manage the stored information and filter the results. However, this means implementing functionalities that Optimis already offers.

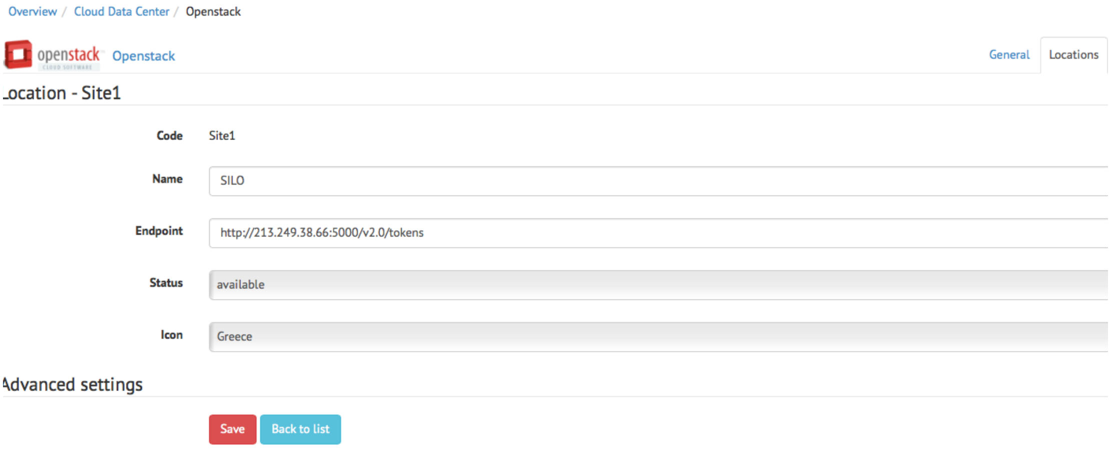
The second approach that was actually followed is the installation of all the needed parts of Optimis Toolkit and the integration with STRATEGIC Service Store through the usage of REST APIs.

The software parts of Optimis needed from STRATEGIC are included in a tool called Infrastructure Provider (IP) Registry. The IP Registry is a standalone web service offered by Optimis and is deployed in a Tomcat application server that is part of STRATEGIC Framework.

Service Store is communicating through REST API to filter target providers that do not fulfil the localization requirements specified at service construction time. This API is called the Service Manifest API[16] and provides a common interface to the Optimis Service Manifest instances. This API used by internal Optimis components but it is also used by STRATEGIC.

Based on the requirements stated in deliverable D2.2[4], one of the main considerations of public bodies is to clarify in which countries personal data will flow and stored during service provisioning of a public service. This will assist the public bodies to ignore specific cloud offerings or use them but implement appropriate safeguards such as using approved standard contractual clauses, binding corporate rules for international data transfer.

Considering the workflow that allows the usage of Optimis, the localisation information that is related to the Infrastructure is provided by the IaaS operator to the Service Store administrator. IaaS operator should provide country metadata when describing their IaaS, during onboarding process. A part of this process is presented in **Figure 10**.



Location - Site1

Code Site1

Name SILO

Endpoint http://213.249.38.66:5000/v2.0/tokens

Status available

Icon Greece

Advanced settings

Figure 10: Example of localization information (country of IaaS) provided during the onboarding process

The information used in the metadata is also used to populate in an automated way through the usage of API, the IP Registry of Optimis.

Public sector administrators that want to use STRATEGIC Service Store can see the geographical information of the IaaS and select what they require but can also provide data protection information about their service, by using Optimis Service Manifest. That information can be stored to the IP Registry again by using the Service Manifest API during deployment time.

[16] https://packcs-e0.scai.fraunhofer.de/service-manifest-snapshot/

The IP Registry service then extracts information from the registry for both the service provider and infrastructure provider, and provides public sector administrator with filtered results.

6 Governance tools

Governance of applications is describing the act of the managing the lifecycle of Services and Workloads deployed through STRATEGIC Service Store. As described in deliverable D4.2a [1], application governance is a task that is mainly addressed by public sector administrators.

However, in this deliverable we will describe the capabilities offered to Service Store operator of STRATEGIC, regarding governance.

6.1 Application governance for Service Store operator

The STRATEGIC Service Store operator has full access to the administrative console of STRATEGIC Service Store. This allows him to have overview of both users and applications. Direct governance of applications deployed by other users is not possible for security reasons by the Service Store operator.

However, it is possible to delegate governance within an organisation by using access management tools offered by STRATEGIC Service Store. This is useful for avoiding using a shared account and connected risks. So, by using this capability Service Store operator can create new users under a specific public sector administrator's account, and then use these users to access Service Store and govern applications in the same way that is executed by public sector administrator. This way, actions made by Service Store operator are non-repudiable, thus allowing public sector administrator to have full knowledge on these actions. After gaining access, governance can be done in the same way that is executed by administrator.

Although not directly related to governance of application, but governance of the STRATEGIC Service Store, Service Store operator is able to manage customer users by creating, removing, updating, and deleting user accounts, as documented in deliverable D4.1a[5]. However all actions executed by Service Store operator are done in a non-repudiable way.

STRATEGIC Service Store operator has the ability to validate a customer account registration. The account needs to be verified with a valid email address from customers, or it can be enabled right away. Moreover, STRATEGIC Service Store operators are able to manage customer users entirely. They are able to create, remove, update, and delete user accounts. Users can be assigned manually to one or more accounts. The consequences of removing users are permanent, so, changes via this channel should be under strict process management.

7 Security tools

7.1 Integration with STORK and SEMIRAMIS

STORK and SEMIRAMIS are two projects that STRATEGIC supports and provides integration with. STORK is providing cross-border authentication and SEMIRAMIS is dealing with cross-country secure attribute exchange. Features of both of the projects are described in detail in D4.3a. Integration is done at the application level, hence only **integrator** level scenario makes sense. This means that in the context of the STRATEGIC project, applications with pre-packaged STORK and SEMIRAMIS components can be distributed.

Given highly specific nature of the extensions (in most cases, application code needs to be adapted) there are no settings for configuration of these applications exposed in STRATEGIC Metadata model. As such, there are no common configuration settings exposed in STRATEGIC Service Store. Instead, integration with STORK and SEMIRAMIS is done based on the created development guides, actual application adaptation and working examples of integrations. The guide for the preparation of the STORK/SEMIRAMIS packages will be delivered as part of D4.3b "Trust and security components" [6].

7.2 BT Intelligent Protection

ISV integrator can create custom protection policies, based on Pen-test & vulnerability analysis, for their custom applications.

IaaS operator can choose to extend the protection capability, by allowing integration at hypervisor level.

Service Store operator can provide the service as a subscription, thus enabling automated protection and security management for all and including multi-cloud deployments.

Public sector administrator can choose the custom level of security for each deployment and will have access to a security dashboard which:

- Summarises state of protection of their multi-cloud deployments;
- Allows for management and policy changes to deployments;
- Create custom roles to allow access to functions like auditors or specialist security specialists to read security event information and operate specified functions.

Managed security provider (a role specific to the BT security features) can manage the security monitoring and event handling for the customer and host the root security management server.

7.3 BT Intelligent Data protection

ISV integrator doesn't have direct function identified. Can recommend protection levels required and the location of various sensitive data created, stored and used by the application.

IaaS operator does not have direct functions identified.

Service Store operator can provide the service as a subscription, thus enabling automated encryption, protection and security management for all and including multi-cloud deployments.

Public sector administrator can choose the custom level of security and the targets to be encrypted and protected in every deployment. Will have access to a security dashboard which

- Manage protection targets;
- Summarises state of protection of their multi-cloud deployments;
- Allows for management and policy changes to deployments;
- Create custom roles to allow access to functions like auditors or specialist security specialists to read security event information and operate specified functions.

Managed security provider can manage the security monitoring and event handling for the customer and host the key management server.

8 Conclusions

This document contains extension of the description of tools and methods for performing typical operations of the target users of STRATEGIC.

Extension was done based on the gap analysis and includes role-based flow description for user actions. In particular:

- Infrastructure on-boarding was described from the perspective of the public sector administrator;
- Application adaptation is covered from the viewpoint of the ISV/Integrator;
- Localization of service deployment taking into account security and legal requirements validated by the integrated Optimis toolkit.
- Application governance is enhanced with user account management by Service Store operator;
- Security components coming from STORK, SEMIRAMIS and BT were described with implications for each of the identified roles.

D4.2b along with D4.2a describes a set of tools comprising STRATEGIC platform toolkit that can be used by WP5 for performing activities related to pilot operations.

9 References

[1] STRATEGIC Deliverable D4.2a Migration, Adaptation, Localization and Governance Tools, 2014

[2] STRATEGIC Deliverable D3.1 Specification of Cloud-Enablement and Migration Solutions and Services, 2014

[3] Optimis D7.2.1.3 Cloud Legal Guidelines, 2012, http://www.optimis-project.eu/sites/default/files/content-files/document/d7213-cloud-legal-guidelines.pdf

[4] STRATEGIC Deliverable D2.2 Pilot Scenarios, Use Cases and Pilot Operations Requirements, 2014

[5] STRATEGIC Deliverable D4.1a STRATEGIC Cloud Broker and Marketplace, 2015

[6] STRATEGIC Deliverable D4.3b Trust and Security components, 2015

I. APPENDIX A: Preparing VM template based on Ubuntu 12.04LTS / 14.04LTS

This section describes how Ubuntu 12.04LTS / 14.04LTS templates are prepared in Apache CloudStack IaaS. Similar process is also followed for other IaaS, like OpenStack. As most steps for preparing Ubuntu 12.04 and Ubuntu 14.04 image are similar therefore most commands are referring to Ubuntu 12.04 but are the same for Ubuntu 14.04.

Import Ubuntu 12.04LTS ISO

An ISO is typically regarded as an OS image, however, you can add ISOs for other types of software. Please do following steps to import Ubuntu 12.04LTS ISO.

1 Login to the CloudStack UI with an admin account.

2 Select Templates tab.

3 In Select View, select *ISOs*.

4 Click on the Register ISO button. System shows *Add ISO* screen. Please fill the data input fields in this page.

- *Name*: Enter the short name for the ISO image. For Ubuntu 12.04LTS, it is *Ubuntu 12.04 (64-bit)*.
- *Description*: Enter the display test description, *Ubuntu 12.04 (64-bit)*, for Ubuntu 12.04.
- *URL*: Enter the URL that hosts the Ubuntu 12.04LTS. The Management Server must be able to access this location via HTTP. If needed you can place the ISO image directly on the Management Server.
- *Zone*: Select the zone where you want the ISO to be available, or All Zones to make it available throughout CloudStack.
- *Bootable*: Tick the Bootable check box to enable gusts to boot off Ubuntu 12.04LTS.
- *OS Type*: Select Ubuntu 12.04 (64-bit) from this drop down list. This helps CloudStack and the hypervisor perform certain operations and make assumptions that improve the performance of the guest. Note If you select an older/newer version of the OS than the version in the image, the image may not work. For example, choosing Ubuntu 12.04 to support a Ubuntu 14.04LTS image will usually not work. In these cases, select *Other Ubuntu (64-bit)*.
- *Extractable*: Select Yes if the Ubuntu 12.04LTS should be available for extraction.
- *Public*: Select Yes if Ubuntu 12.04LTS should be available to other users.

- *Featured*: To flag Ubuntu 12.04LTS as a featured ISO, please select Yes. The ISO will appear in the Featured ISOs list. Note than only an administrator can mark an ISO as Featured.

5 Click on the OK button. The Management Server will download Ubuntu 12.04LTS. Downloading may take a several minutes based on the file size and internet connectivity speed. The ISO status column displays *Ready* when Ubuntu 12.04LTS is successfully downloaded into secondary storage.

Warning

Wait for the ISO to finish downloading. If you move on to the next task and try to use the ISO right away, it will appear to fail. The entire ISO must be available before CloudStack can work with it.

Launch VM from Ubuntu 12.04LTS ISO

CloudStack allows you to launch VM from Ubuntu 12.04LTS ISO. This feature helps receiving monitoring services via a shared network provided by a service provider for the VMs deployed in a multi-tier application. Please do following steps to launch VM from Ubuntu 12.04LTS ISO.

1 Log in to the CloudStack UI as an administrator.

2 Select Instances tab.

3 Click on the +Add Instances button.

4 Select the Zone and then click the Next button.

5 Select the ISO just uploaded and then click the Next button. System shows *Compute Offering*.

6 In the Compute Offering section, enter at least *1 vCPU* and *2GB RAM*. Click the Next button. System shows Data Disk Offering.

7 In the Data Disk Offering section, enter at least *20GB* disk space. Click the Next button.

8 In the Network tab, enter 2 NICs. Default network should be Isolated network and second one is Shared network. Click the Next button.

9 Enter the VM Name.

10 Click on Launch VM.

Install Ubuntu 12.04TLS on VM

You can install Ubuntu 12.04LTS on VM. Please do following steps to install Ubuntu 12.04LTS on VM.

1 Log in to the CloudStack UI as a user or admin.

2 Select Instances tab.

3. Select the name of a running *VM*.
4. Click on the View Console icon.
5. Setup Ubuntu 12.04LTS with default settings.

Install XenServer tools

You can install XenServer on VM. Please do following steps to install XenServer on VM.

1. Log in to the CloudStack UI as a user or admin.
2. Select Instances tab.
3. Click on the Detach ISO icon.
4. Attach xs-tools.iso.
5. Log in to the VM using CS UI and then run following command.

```
sudo su -

cd /mnt

mkdir xs-tools

mount /dev/cdrom /mnt/xs-tools/

cd /mnt/xs-tools/Linux/

dpkg -i *amd64.deb

cd /
```

Delete default account in Ubuntu 12.04LTS (Optional)

Set root password to some known password so that you can login back to delete the cloud default account.

1. You can delete users from our Ubuntu 12.04LTS with the command *userdel* The correct syntax is "userdel [options] username". To remove user home directory and mail spool add parameter -r as option. userdel -r "user-name"

2. Check that home directory and mail spool was removed: [root@ubuntu ~]# ll /var/spool/mail/

   ```
   total 0

   [root@ubuntu ~]# ll /home/

   total 0
   ```

3. Logout and login with root account.

Enable Password Management to Your Templates part

CloudStack provides an optional feature that allows users to set temporary admin or root password reset. This feature also allows you to reset an existing admin or root password from the UI. You may need to download additional scripts to cope-up with your template in order to enable this feature. You can instruct the system whether reset admin/root password feature should be enabled for the new template.

The password management capability resets the password of the account on instance boot as well as the script does an HTTP call for retrieving account password to the router that should be reset. The guest can access the account password until they have access to virtual router. The virtual router receives the password from the management server when you request a password reset. This process enforces an instance reboot in order to effect the password change. Note that if the script is unable to contact the virtual router during instance boot, it will not set the password but boot will continue normally.

Please do following steps to add password management to your templates part.

```
apt-get update

apt-get -y install whois

wget http://download.cloud.com/templates/4.2/bindir/cloud-set-guest-password.in -O /etc/init.d/cloud-set-guest-password

chmod +x /etc/init.d/cloud-set-guest-password

ln -s /etc/init.d/cloud-set-guest-password /etc/network/if-up.d/cloud-set-guest-password

ln -s /etc/init.d/cloud-set-guest-password /etc/network/if-down.d/cloud-set-guest-password
```

Install and configure Cloud-init in VM - Ubuntu 12.04

Ubuntu 12.04 and 14.04 have similar steps to install custom cloud-init, except there are a couple of extra steps with Ubuntu 12.04. To install custom cloud-init, please do following steps.

1 Execute following code: cat << "EOF" > /etc/apt/preferences.d/rightscale-cloud-init-pin-1001

```
Package: cloud-init

Pin: version 0.7.2*

Pin-Priority: 1001
```

2 Execute the following code: curl http://mirror.rightscale.com/rightlink/rightscale.pub | apt-key add -

3 echo "deb [arch=amd64] http://mirror.rightscale.com/rightscale_software_ubuntu/latest precise main" > /etc/apt/sources.list.d/rightscale_extra.sources.list

```
4   apt-get -y update
5   apt-get -y --force-yes install cloud-init python-serial
```

Create configuration file

```
cat << "EOF" > /etc/cloud/cloud.cfg.d/99_CloudStack.cfg
```

Add inside the file:

```
datasource:
  CloudStack: {}
  None: {}
datasource_list:
  - CloudStack
```

Edit configuration file cat << "EOF" > /etc/cloud/cloud.cfg, as follows

```
datasource_list: ["CloudStack"]
# The top level settings are used as module
# and system configuration.

# A set of users which may be applied and/or used by various modules
# when a 'default' entry is found it will reference the 'default_user'
# from the distro configuration specified below
users:
   - default

# If this is set, 'root' will not be able to ssh in and they
# will get a message to login instead as the above $user (ubuntu)
disable_root: true

# This will cause the set+update hostname module to not operate (if true)
preserve_hostname: false

# Example datasource config
# datasource:
#    Ec2:
#      metadata_urls: [ 'blah.com' ]
#      timeout: 5 # (defaults to 50 seconds)
#      max_wait: 10 # (defaults to 120 seconds)

# The modules that run in the 'init' stage
cloud_init_modules:
 - migrator
 - bootcmd
 - write-files
 - growpart
 - resizefs
 - set_hostname
 - update_hostname
 - update_etc_hosts
 - ca-certs
 - rsyslog
 - users-groups
 - ssh

# The modules that run in the 'config' stage
cloud_config_modules:
# Emit the cloud config ready event
# this can be used by upstart jobs for 'start on cloud-config'.
 - emit_upstart
 - mounts
 - ssh-import-id
 - locale
 - grub-dpkg
 - apt-pipelining
 - apt-configure
 - package-update-upgrade-install
 - landscape
 - timezone
 - puppet
 - chef
 - salt-minion
 - mcollective
 - disable-ec2-metadata
 - runcmd
 - byobu

# The modules that run in the 'final' stage
cloud_final_modules:
 - rightscale_userdata
 - scripts-per-once
 - scripts-per-boot
 - scripts-per-instance
 - scripts-user
 - ssh-authkey-fingerprints
 - keys-to-console
 - phone-home
 - final-message
 - power-state-change

# System and/or distro specific settings
# (not accessible to handlers/transforms)
system_info:
  # This will affect which distro class gets used
  distro: ubuntu
  # Default user name + that default users groups (if added/used)
  default_user:
      name: ubuntu
      lock_passwd: True
      gecos: Ubuntu
      groups: [adm, audio, cdrom, dialout, floppy, video, plugdev, dip, netdev]
      sudo: ["ALL=(ALL) NOPASSWD:ALL"]
      shell: /bin/bash
  # Other config here will be given to the distro class and/or path classes
  paths:
      cloud_dir: /var/lib/cloud/
      templates_dir: /etc/cloud/templates/
      upstart_dir: /etc/init/
  package_mirrors:
      - arches: [i386, amd64]
        failsafe:
            primary: http://archive.ubuntu.com/ubuntu
            security: http://security.ubuntu.com/ubuntu
        search:
            primary:
              - http://%(ec2_region)s.ec2.archive.ubuntu.com/ubuntu/
              - http://%(availability_zone)s.clouds.archive.ubuntu.com/ubuntu/
            security: []
      - arches: [armhf, armel, default]
        failsafe:
            primary: http://ports.ubuntu.com/ubuntu-ports
            security: http://ports.ubuntu.com/ubuntu-ports
  ssh_svcname: ssh
```

Install and configure Cloud-init in VM - Ubuntu 14.04

To install custom Ubuntu 14.04 in cloud-init please do following steps.

1 Execute following code: curl http://mirror.rightscale.com/rightlink/rightscale.pub | apt-key add -

2 echo "deb [arch=amd64] http://mirror.rightscale.com/rightscale_software_ubuntu/latest trusty main" > /etc/apt/sources.list.d/rightscale_extra.sources.list

3 apt-get -y update

4 apt-get -y --force-yes install cloud-init python-serial

5 Edit configuration file cat << "EOF" > /etc/cloud/cloud.cfg

```
datasource_list: ["CloudStack"]
user: root
disable_root: 0
ssh_pwauth: 1
preserve_hostname: False

cloud_init_modules:
 - bootcmd
 - resizefs
 - set_hostname
 - update_hostname
 - update_etc_hosts
 - ca-certs
 - rsyslog
 - ssh

cloud_config_modules:
 - disk-setup
 - mounts
 - ssh-import-id
 - locale
 - grub-dpkg
 - apt-pipelining
 - apt-update-upgrade
 - landscape
 - timezone
 - puppet
 - chef
 - salt-minion
 - mcollective
 - disable-ec2-metadata
 - runcmd
 - byobu

cloud_final_modules:
 - rightscale_userdata
 - scripts-per-once
 - scripts-per-boot
 - scripts-per-instance
 - scripts-user
 - keys-to-console
 - phone-home
 - final-message

system_info:
  package_mirrors:
      - arches: [i386, amd64]
        failsafe:
            primary: http://archive.ubuntu.com/ubuntu
            security: http://security.ubuntu.com/ubuntu
        search:
            primary:
              - http://%(ec2_region)s.ec2.archive.ubuntu.com/ubuntu/
              -
http://%(availability_zone)s.clouds.archive.ubuntu.com/ubuntu/
```

```
        security: []
    - arches: [armhf, armel, default]
      failsafe:
        primary: http://ports.ubuntu.com/ubuntu-ports
        security: http://ports.ubuntu.com/ubuntu-ports
```

Cleanup Part (Optional)

It is good practice to cleanup path by executing:

1 To clean APT cache and temp file: sudo apt-get clean all

2 rm -rf /tmp/*

3 To clear user history, clear the bash command rm -f ~/.bash_history

4 unset HISTFILE

5 history -c

Build Image based on VM

You can build Image based on virtual machine. Please do following steps to build Image based on the VM.

1 Log in to the CloudStack UI as a user or admin.

2 Select Instances tab.

3 Select the running VM.

4 Click on the View Volumes option.

5 Click on the Root Disk.

6 Click on the Create Template icon. System shows data input fields.

7 Enter *Ubuntu12.04 (64-bit)* in the Name field.

8 Enter *ubuntu12.04 (64-bit)* in the Description field.

9 Select the OS Type.

10 Tick the Password Enabled check box to enable password protection.

Add tag to Template

Ubuntu Template Tagging

Key	Value

used_by	servicestore
ostype	ubuntu
version	12.04 (or 14.04 for Ubuntu 14.04 template)
bootstrap_method	cloudinit

Launch VM in STRATEGIC Service Store

To launch VM in STRATEGIC Service Store, you need to synchronize it first. Then you can launch the app. Please do following steps to launch VM in STRATEGIC Service Store.

1 Login to the system as account administrator.

2 Select Synchronize option from the Settings.

Now you can launch the Ubuntu from the Launch page. Please refer the step by step process for Launch application help page

II. APPENDIX B: Preparing VM template based on CentOS

This section describes how CentOS templates are prepared in Apache CloudStack IaaS. Similar process is also followed for other IaaS, like OpenStack.

ISO images can be added to an IaaS in case needed to enable additional OS/software available for use with guest VMs. An ISO is typically regarded as an OS image, however, you can add ISOs for other types of software. In this section you can understand how Centos 6.5 ISO is imported to the system. Please do following steps to import Centos 6.5 ISO.

1 Login to the CloudStack UI with an admin account

2 Select Templates tab.

3 In Select View, select *ISOs*.

4 Click Register ISO button. System shows Add ISO screen. Plase fill the data input fields in this page.

- *Name*: Enter the short name for the ISO image. For Centos 6.5, itis *Centos 6.5 (64-bit)*.
- *Description*: Enter the display test description, *Centos 6.5 (64-bit)*, for Centos 6.5.
- *URL*: Enter the URL that hosts the Centos 6.5. The Management Server must be able to access this location via HTTP. If needed you can place the ISO image directly on the Management Server.
- *Zone*: Select the zone where you want the ISO to be available, or All Zones to make it available throughout CloudStack.
- *Bootable*: Tick the Bootable check box to enable gusts to boot off CentOS 6.5.
- *OS Type*: Select Centos 6.5 (64-bit) from this drop down list. This helps CloudStack and the hypervisor perform certain operations and make assumptions that improve the performance of the guest. Note If you select an older/newer version of the OS than the version in the image, the image may not work. For example, choosing CentOS 5.4 to support a CentOS 6.5 image will usually not work. In these cases, select *Other Centos (64-bit)*.
- *Extractable*: Select Yes if the CentOS 6.5 should be available for extraction.
- *Public*: Select Yes if CentOS 6.5 should be available to other users.
- *Featured*: To flag CentOS 6.5 as a featured ISo, please select Yes. The ISO will appear in the Featured ISOs list. Note than only an administrator can mark an ISO as Featured.

5 Click on the OK button. The Management Server will download CentOS 6.5. Downloading may take a several minutes based on the file size and

internet connectivity speed. The ISO status column displays *Ready* when CentOS 6.5 is successfully downloaded into secondary storage.

6 Wait for the ISO to finish downloading. If you move on to the next task and try to use the ISO right away, it will appear to fail. The entire ISO must be available before CloudStack can work with it.

Launch VM from Centos 6.5 ISO

CloudStack allows you to launch VM from Centos 6.5 ISO. This feature helps receiving monitoring services via a shared network provided by a service provider for the VMs deployed in a multi-tier application. Please do following steps to launch VM from Centos 6.5 ISO.

1 Log in to the CloudStack UI as an administrator.

2 Select Instances tab.

3 Click on the +Add Instances button.

4 Select the Zone and then click the Next button.

5 Select the ISO just uploaded and then click the Next button. System shows *Compute Offering*.

6 In the Compute Offering section, enter at least *1 vCPU* and *2GB RAM*. Click the Next button. System shows Data Disk Offering.

7 In the Data Disk Offering section, enter at least *20GB* disk space. Click the Next button.

8 In the Network tab, enter 2 NICs. Default network should be Isolated network and second one is Shared network. Click the Next button.

9 Enter the VM Name.

10 Click on Launch VM.

Install Centos 6.5 on VM

You can install Centos6.5 on VM. Please do following steps to install Centos 6.5 on VM.

1 Log in to the CloudStack UI as a user or admin.

2 Select Instances tab.

3 Select the name of a running *VM*.

4 Click on the View Console icon.

5 Setup centos 6.5 with default settings.

Install XenServer tools

You can install XenServer on VM. Please do following steps to install XenServer on VM.

1 Log in to the CloudStack UI as a user or admin.

2 Select Instances tab.

3 Click on the Detach ISO icon.

4 Attach xs-tools.iso.

5 Log in to the VM using CS UI and then run following command.

```
sudo su -

cd /mnt

mkdir xs-tools

mount /dev/cdrom /mnt/xs-tools/

cd /mnt/xs-tools/Linux/

bash install.sh
```

Delete default account in Centos 6.5 (Optional)

Set root password to some known password so that we can login back to delete the cloud default account.

1 You can delete users from our Centos 6.5 with the command *userdel* The correct syntax is "userdel [options] username". To remove user home directory and mail spool add parameter -r as option. userdel -r "user-name"

2 Check that home directory and mail spol was removed:

```
[root@centos1 ~]# ll /var/spool/mail/

total 0

[root@centos1 ~]# ll /home/

total 0
```

3 Logout and login with root account.

Adding Password Management to Your Templates part

CloudStack provides an optional feature that allows users to set temporary admin or root password reset. This feature also allows you to reset an existing admin or root password from the UI. You may need to download additional scripts to cope-up with your template in order to enable this feature. You can instruct the system whether reset admin/root password feature should be enabled for the new template.

The password management capability resets the password of the account on instance boot as well as the script does an HTTP call for retrieving account password to the router that should be reset. The guest can access the account password until they have access to virtual router. The virtual router receives the password from the management server when you request a password reset. This process enforces an instance reboot in order to effect the password change. Note that if the script is unable to contact the virtual router during instance boot, it will not set the password but boot will continue normally.

Please do following steps to add password management to your templates part.

```
wget http://download.cloud.com/templates/4.2/bindir/cloud-set-guest-password.in -O /etc/init.d/cloud-set-guest-password

chmod +x /etc/init.d/cloud-set-guest-password

chkconfig --add cloud-set-guest-password
```

User-Data and Meta-Data part: Use *Cloud-Init*

You can use Cloud-Init to access an interpret user-data from virtual machines. Cloud-Init to be installed into templates as well as it requires CloudStack password and sshkey scripts. Note that cloud-init does not support *User password management* and *resetSSHKeyForVirtualMachine* API at present. Please do following steps to use Cloud-Init.

1 Install cloud-init package into a template:

```
yum list updates

yum install cloud-init
```

2 Create configuration file: /etc/cloud/cloud.cfg.d/99_CloudStack.cfg

```
cat << "EOF" > /etc/cloud/cloud.cfg.d/99_CloudStack.cfg

 datasource :

 CloudStack: {}

 None: {}

datasource_list:

 - CloudStack
```

3 Edit configuration file: /etc/cloud/cloud.cfg file

```
cat << "EOF" > /etc/cloud/cloud.cfg

datasource_list: ["CloudStack"]

user: root

disable_root: 0

ssh_pwauth: 1

preserve_hostname: False


cloud_init_modules:

 - bootcmd

 - resizefs
 - set_hostname
 - update_hostname
 - update_etc_hosts
 - ca-certs
 - rsyslog
 - ssh

cloud_config_modules:
 - disk-setup
 - mounts
 - ssh-import-id
 - locale
 - grub-dpkg
 - apt-pipelining
 - apt-update-upgrade
 - landscape
 - timezone
 - puppet
 - chef
 - salt-minion
 - mcollective
 - disable-ec2-metadata
 - runcmd
 - byobu

cloud_final_modules:
 - rightscale_userdata
 - scripts-per-once
 - scripts-per-boot
 - scripts-per-instance
 - scripts-user
 - keys-to-console
 - phone-home
 - final-message

system_info:
  package_mirrors:
      - arches: [i386, amd64]
        failsafe:
            primary: http://archive.ubuntu.com/ubuntu
            security: http://security.ubuntu.com/ubuntu
        search:
            primary:
              - http://%(ec2_region)s.ec2.archive.ubuntu.com/ubuntu/
              - http://%(availability_zone)s.clouds.archive.ubuntu.com/ubuntu/
            security: []
      - arches: [armhf, armel, default]
        failsafe:
            primary: http://ports.ubuntu.com/ubuntu-ports
            security: http://ports.ubuntu.com/ubuntu-ports
```

Cleanup Part (Optional)

It is good practise to cleanup part. To cleanup part:

1. To clean network interface configuration file: rm **-**f **/**etc**/**sysconfig**/**network**-**scripts**/**route**-**eth1
2. To clean YUM cache and temp file: /usr/bin/yum clean all
3. rm -rf /tmp/*
4. To clear user history, clear the bash command rm -f ~/.bash_history
5. unset HISTFILE
6. history -c

Build Image based on VM

You can build Image based on virtual machine. Please do following steps to build Image based on a running VM.

1 Log in to the CloudStack UI as a user or admin.

2 Select Instances tab.

3 Select the running VM.

4 Click on the View Volumes option.

5 Click on the Root Disk.

6 Click on the Create Template icon. System shows data input fields.

7 Enter *Centos6.5 (64-bit)* in the Name field.

8 Enter *Centos6.5 (64-bit)* in the Description field.

9 Select the OS Type.

10 Tick the Password Enabled check box to enable password protection.

Add tag to Template

Centos Template Tagging

Key	Value
used_by	servicestore
ostype	centos
version	6.5
bootstrap_method	cloudinit

Launch VM in STRATEGIC Service Store

To launch VM in STRATEGIC Service Store, you need to synchronize it first. Then you can launch the app. Please do following steps to launch VM in STRATEGIC Service Store.

1 Login to the system as account administrator.

2 Select Synchronize option from the Settings.

Now you can launch the Centos from the Launch page