EGI Federated Cloud Check-in/AppDB

Baptiste Grenier / Enol Fernández

with material from Nicolas Liampotis and Marios Chatziangelou



EGI-Engage is co-funded by the Horizon 2020 Framework Programme of the European Union under grant number 654142



www.egi.eu



- Multi-cloud IaaS with Single Sign-On via Check-In
- Technology agnostic:
 - OpenStack,
 - OpenNebula
 - Synnefo

EGI Cloud Federation



The infrastructure







EGI Compute services

	EGI Cloud Compute	EGI Cloud Container Compute	EGI High Throughput Compute
What is it?	Multi-cloud IaaS	Kubernetes on top of EGI Cloud Compute	The grid, a scalable batch system
What you run?	VMs	(Docker) Containers	Jobs
Typical workloads	Lift and shift existing applications Specific OS (kernel) requirements	Cloud-native containerised applications.	Execution of parallel computing tasks to analyse large datasets.
Pros / Cons	[+] Complete control on resources, run (almost) anything you'd like[-] Complex operation	 [+] Industry standard [+] Hides complexity of Kubernetes setup [-] Some Kubernetes features not available 	 [+] No management of resources, just submit jobs [-] Legacy interfaces [-] Porting of applications
	Configurability		Abstraction

EGI Cloud Compute



- Run Virtual Machines on demand on EGI's Cloud Federation
 - Similar to AWS EC2/EBS or GCP Compute Engine
- Diverse providers with common:
 - AuthN and AuthZ
 - VM Image catalogue
 - Information discovery
 - Accounting
 - Monitoring
 - GUI dashboard

EGI Cloud Compute – the basics



www.egi.eu



Users

A multi-cloud IaaS for research

Providers

- Single-Sign On via Check-in
- Appliance Library
- Resource discovery
- Single GUI dashboard
- Computation near data

- Support international communities
- Operational and security processes
- A/R Monitoring
- Accounting
- Technology agnostic



Integration with resource providers

- Providers keep complete control on their resources
 - Enable access to a Virtual Organisation into local projects with EGI credentials, SLA based
 - Set of extra components using OpenStack APIs to retrieve provider information and make it available to EGI services
- No (major) changes in operational activities
 - Provide support through EGI channels
 - Comply with the operational and security procedures. These are based on best practices and common requirements
 - Most well-operated providers already have these activities in place, so the additional task for a site manager is to acknowledge to EGI that the task has been performed.



VO 1 (cloud a, b, c)

(cloud b, c, d, e, f)

- Community-specific VOs e.g. CHIPSTER, Highthroughtputseq, EISCAT, etc. (SLA, OLAS)
- 2. Training VO = training.egi.eu
- 3. Generic VOs e.g. fedcloud.egi.eu \rightarrow Incubator for new users

VO 2

Browse VOs at http://operations-portal.egi.eu/vo/search (both HTC and cloud)

www.egi.eu





Identity and Access Management solution that makes it easy to secure access to services and resources



Components

- IdP/SP Proxy
- User enrolment & group management
- IdP Discovery
- Token Translation

Documentation

- Usage guide
- Integration guides

https://wiki.egi.eu/wiki/AAI



What benefits does Check-in bring?

Single sign-on to services through eduGAIN, social media and other institutional or communitymanaged identity providers

Only one account needed for federated access to multiple heterogeneous (web and non-web) service providers using different technologies (SAML, OpenID Connect, OAuth 2.0, X509)

Identity linking enables access to resources using different login credentials (institutional/social)

Assurance information associated to each authenticated identity

Aggregation and harmonisation of authorisation information (VOs/groups, roles, assurance) from multiple sources





- Implementation of the AARC blueprint architecture
- Registered in eduGAIN as an SP complying with REFEDS Research & Scholarship and Sirtfi
- All community SPs can have one statically configured IdP
- No need to run an IdP Discovery Service on each community SP
- Connected SPs get consistent/harmonised user identifiers and accompanying attribute sets from different IdPs/AAs that can be interpreted in a uniform way for authorisation purposes



Integration of OpenStack with Check-in

- OpenID Connect (OIDC)
 - Industry standard
 - Web and non-web friendly (OAuth2.0)
 - Supported by OpenStack since Icehouse
- OpenStack Providers need to:
 - 1. Configure OpenStack support for OIDC (supported upstream)
 - 2. Add EGI Check-in as IdP for OpenStack
 - 3. Configure mapping of Check-in users to local projects as agreed with VOs







G Marcalast Harles	ferm X +			
00 00	No.lookajaches/costination		A fact	n. 1
Applica	tions Database	Sature C	nud urterplace People	
Cloud Mp	(Search in without appliances,	9.0	Instant - Descript -	
to text	Films: other per work (*			D
Real Value Recently (colonal	10.10		11 martia - 120	E
M obgelænsen Application Desempresen Application Benærs		(build from 100175	, ,	-
Application Station Registers	80 anticest (burs, 1434 (%		Magnetic galaxies and the second state of the	-
Rostrass Apps Collaboration Contact: Apps	A fraction	A fourtait	A Starting	
Destroyer & Carring	Long Statutes lies	0-	name and the second	
Conception Appen				

Registry for virtual appliances (VA) ✓ a logical container of versioned image file & metadata bundles

Registry for software appliances

 a logical container of VA versions & contextualization scripts bundles

VA distribution medium

✓ distributing endorsed VAs to the resource providers/sites



AppDB – Cloud Marketplace (2)

Resource providers catalogue

 list of the VAs which are available by each site/resource provider

Virtual Organizations (VO) catalogue

 ✓ list of the VAs which are available for each VO member





AppDB – a browsable information system

ET Envil

VD diffectence.org

C . 5ec

100.

51	te: UPV-GRYC/	AP (ES)				•	二五十 四
54	H: IN2P3-IRES	(FR)					
	Image: ver.1.7 Uburtu 14.04/x88_84/VHueBox +						le
	Memory	Disk	Logical Physical CPUs	Connectivity In/Out	OS Family		
	612000	160 GB	4548	yesiyes	linux	get IDs	
	252144	320-08	16/16	yesiyes	linux.	pet iCu	4
	282144	50 GB	16/16	yesiyes	linux.	pet iCh	
	131072	50 GB	16/16	yes/yes	Sinux.	get iCu	
	131072	80 GB	16/16	yesiyes	linux.	get iCu	
	131072	320-08	16/16	yes/yes	linux.	get iCu	
	65536	80 G/B	30/52	yesiyes	linux.	get IDs	
	65536	80 GB	16/16	yes/yes	linux.	get iDu	
	32768	320-08	16/16	yesiyes	linux.	get iCu	
	16384	160-OB	88	yes/yes	linux.	pet IDs	
	8192	80 G/B	44	yesiyes	linux.	pet ID4	
	4096	20.08	22	yesiyes	linux.	get Ets	
	4096	40.08	22	yesiyes	Briuk	get (Dis	
	4096	20 08	57	yesiyes	limux.	get iCh	
	2048	20 GB	57	yesiyes	linux.	get iCu	
	2048	50 GB	9/9	yesiyes	linux.	pet iCu	
	812	1.08	57	yesiyes	firmum.	get (Da	Galicia
54	te: SCAI (DE)						

6/28/18



AppDB – a GraphQL powered information system

More information at https://docs.google.com/presentation/d/19Yh3kNxl01DfcrDgQf12w-KOW5Zrd_OnYP2iGp9Kg2Y/edit?ts=5a2ab515#slide=id.p

0 0 0 / D Banks. + (11)		\$7 End
C O Not Secure is mark helaspid providy schiption	-1095645295264666666666666658452952952952952952952952952952952952952	X 1
GraphiQL (Putty Heavy		Cocs
<pre>1 = { 2 = { 3</pre>	<pre>{ "deta": { "initializervices": { "subset:ELT: "https://feekiewi-services.spi.cemps.es:1548 "subset:ELT: "https://seci.cloud.godg.de:3580", "subset:ELT: "https://seci.subs.sk:ETE7/secil.1", "subset:ELT: "https://seci.subs.sk:ETE7/secil.1", "subset:ELT: "https://seci.subs.sk:ETE7/secil.1", "subset:ELT: "https://seci.subs.sk:ETE7/secil.1", "subset:ELT: "https://seci.subs.sk:ETE7/secil.1", "subset:ELT: "https://stack-server.ct.infn.it:ETE7/secil.1", "subset:ELT: "https://stack-server.its.secil.445", "subset:ELT: "https://stack-server.its.secil.445", "subset:ELT: "https://stack-server.its.secil.445", "subset:ELT: "https://stack-server.its.secil.445", "subset:ELT: "https://stack-server.its.secil.445", "subset:ELT: "https://stack-server.its.secil.445",</pre>	e r.
STORY REPORTS	100 · · · ·	

CloudKeeper: AppDB integration

APPLICATION CONTRACTOR

The Device Use definition to a table predicted in recognition of reproduction pattern annual that the second of the Tell Distortion Uses THES, The Tell'Indian Tell Tell

A Production of the	et tout		
B Texas Man (applied approximation) and a	+ 1.0.1		
Aller Grant Calabane Set Set Set Set Set Set Set Set Set Se	44-1-144 (44	- ar Ob	
Receipt Fallance? What haples receipt (server) & harpy		cloudkeener	
Bioloncol 2 marks 2 parks 2 parks 4 pa	Name of Control of Con	Cloud Keeper	ngole (10.000 kil) di di di Latania (10.000 kil) di la 2 Marina di Latania (10.000 kil) di latania (10.000 kil) di latania (10.000 kil) di latania (10.000 kil) di latani Interna
		[CentOS/7/VirtualBox]	
		nee Inage	Security
 cloudkeeper ensures: Integrity of images Conversion to appropriate forr Correct metadata info at glanc 	nats e	Australiante de la construction de la construction de la construction de la construcción	Ann Ann Anthraid a' Airdine Ann Ann Ann Ann Ann Ann Ann Ann Ann Ann
•		MARKA STOCKARD AND A CONTRACT AND A	in the

www.egi.eu

1 1 1

SI Igi.eu		eshboard x	Ivia	nage	: \		o via A	pbr	Check-in integration
Vizard-like	← → C ▲	Secure https://deshboard.ap Dashboard VHCDpensions Topologies All of your topolo	pdb.egi.eu /vrops/topo gies	ologies			Cloud availability	🖈 🌸 🕹 其	ello •
VMs		Q. Surch.					search 0¢	(< 100.848 >	Single
	A state	Name	Virtual Organization	active 🖾	vm #	syed by user	undeployed by infrastructure Created At V	Updated At	dashboard for all providers
		flannel	ve.access.egi.eu	CESGA	з	O running	2018-06-20.06:31:52	2018-06-20-07-27:00	
	Winteron	newkub	vo.access.egi.eu	CESGA	3	O running	2018-06-19 10:21:27	2018-06-19 10:25:44	
		kubernetes	va.access.egi.eu	I INFN-CATANIA-	4	e running	2018-06-15 06:44:06	2018-06-15-06:46:50	
		extra_rode	va.access.egi.eu	CESGA	1	e running	2018-06-15 06:30:54	2018-06-15-06-52:01	
		EGI. CentOS. 7	fedcloud.egi.eu	CESNET-MetaCA	1	e running	2018-06-14 12:40:53	2018-06-14 12:43:45	
						a superior	2018-05-2512-42-22	2058-05-25 12:45:30	
		integrated	fedcloud.egi.eu	CESNET-MetaCl	1	0 running	2010-07-27 12-12-32	2202 07 27 12 12 10 10	
		integrated EGLUburita_56,04,075	fedcloud.egi.eu fedcloud.egi.eu	EESNET-MetaCl	1	e running	2018-02-26 11:54:40	2018-02-26 12 12 18	



Architecture







API access: dealing with heterogeneity

- EGI Federated Cloud no longer mandates a single API for every provider
 - OCCI still widely supported but sites are moving native APIs (mainly OpenStack!)
- Tools to deal with heterogeneity:
 - IaaS orchestration tools with support for multiple APIs:
 - Infrastructure Manager, Terraform, OCCOPUS, ...
 - <u>https://wiki.egi.eu/wiki/Federated_Cloud_laaS_Orchestration</u>
 - IaaS libraries with support for multiple APIs:
 - libcloud, jclouds,...
 - See guide on migrating from OCCI to IM on EGI's wiki: <u>https://wiki.egi.eu/wiki/Federated Cloud OCCI to IM Migration</u>

Containers



- Containers provide virtualisation at the OS level
 - Same kernel, isolated user-space
 - Faster deployment, less overhead, easier migration...





Container orchestration





EGI Cloud Container Compute

- Run containers on top of EGI Cloud Compute VMs
- 2 (+ 1) options:
 - Single node: start the EGI Docker VM and run containers directly (or with docker compose)
 - Kubernetes: start a cluster of VMs and create a Kubernetes cluster to run your containers
 - Start the cluster using IM + Ansible
 - Working on: auto-scaling with EC3, Check-in integration at Kubernetes level
 - udocker: run containers as jobs in the EGI HTC service
 - https://wiki.egi.eu/wiki/Federated_Cloud_Containers



New models for the EGI Cloud

Provide feedback on the proposal at http://go.egi.eu/egi-cloud-expansion

- Lighter federation to attract providers and users
 - Introduce new types of services and resources
 - Marketplace oriented
 - 3 different models under discussion
 - Application Services
 - IaaS Alliance
 - Applications Platforms
- Objectives
 - Facilitate innovation
 - Make it easier for providers to enter the EOSC landscape
 - Offer a broader set of services for users

Under development: EGI Notebooks

- Offer Jupyter notebooks
 'as Service'
 - One-click solution, just login and start using
- EGI Features:
 - Login with Check-in
 - Persistent storage
 - Bring your own environments/kernels
 - Use EGI computing and storage resources from your notebooks

📁 Jupyter					
	Sign in with EG Checkin				
	1 japana hariat Makuda	0	0		0 .
jupyter	1 japana bahad matsuda.	¢	0 See	Carried Par	0 14
jupyter	1 japana bahad matsadas	¢	0 Laper	© Denina Par	•
jupyter Tas Runny Dates	a gayan di balkud (balkud si	¢	0 Lagua	October Par	0
Jupyter Tas Buring Datas Materians in palana Intern	a gayan di balkud (balkud si	¢	0 Laper	Control Far	
Jupyter Tes Buring Dates Melal lens is poten action on tem	i jagenist helinat filetinal sc	¢	0 Lopel Tere 8	Control For Last Name - Last Model	-





 Federated Cloud at EGI wiki: <u>https://wiki.egi.eu/wiki/EGI_Federated_Cloud</u>

- Installation manual: <u>http://egi-federated-cloud-integration.readthedocs.io/</u>
- EGI Federated Cloud list: fedcloud-tf@mailman.egi.eu

Thank you for your attention.

Questions?



This work by Parties of the EGI-Engage Consortium is licensed under a <u>Creative Commons Attribution 4.0 International License</u>.



www.egi.eu



Token translation – Integration with RCauth.eu Online CA

- Check-in has been integrated with the production RCAuth.eu Online CA
 - Users can retrieve X.509 proxies by authenticating through Check-in
 - Check-in Master Portal retrieves end-entity certificate from RCauth.eu
 - Long-lived proxy certificate stored in backend MyProxy server
 - Short-lived proxies provided via:
 - Science Gateways via OIDC (socalled VO-portals)
 - users e.g. via SSH key authentication





User enrolment & group management

- Ability to create enrolment flows specific to a community's requirements
- Support for oganising users in hierarchical groups
- Ability to associate certificate and ssh key information to researcher's federated identity
- Ability to enrich researcher's identity with community-specific attributes
- Direct (de)provisioning of information into an LDAP directory or VOMS

My	Community		
± 6.	Sign Up	•	Enrolment Flow
	Complete the sign-up I	term by antening all the required fields	Collect Petitionan Attributes
	***		Anguani Jinal Address Confirmation Mail for Confirmation
	Name [®] Nor following	See See 4	Confirm Small Address Record Menther Process Confirmation
		Specify Startes	Proving .

Harden - Mar Carefording - No Paparater - 12 Parat - Namopa Song Harden And

Manage Jane Doe Group Memberships

- Name	200700			1000	
COudmins.	My Community Administration	Cost	104	Wenter	(here)
COCILIAR alters	AND NOTIFICATION OF A	Cost	Ac. 14	Warrison	lars.
COCCULARE renters ache	HARE NOTICE METRICES	-Crosell	Actual	- Norther	(server
Strictle Additional Advantages of	464E Members	Creed	Activ	- Merther	(berner
(COmpress) all the	operated. Addresses along	Crowl	404	Wenter	(here)
(2) Citizgeners renders whe	opmore Active Members	Crowl	Actes	Warder	(and
CO Chargement metherical	spenors Rentant	Cost	A-1140	- Marriage	(and
COCTORE an orthographies	test can configered televisioners	Casel	Atta	Warder	Dere
O'Climes as ordered renterative	tel se coñuna tube Verties	-Crosell	A046	wenter	(server
(COnstant on order or metarcal	test oso-confluence Members	Creek	Actie	Warder	(berner
Contraction of the second second	and one of the statement and	-		-	-





www.egi.eu



Group membership and role information

Use of URN-formatted entitlement values based on AARC guidelines:

urn:mace:egi.eu:group:<group>[:<subgroup>*][:role=<role>]#<group-authority>

- <group> is the name of a VO, research collaboration or a top level arbitrary group; unique within a given <namespace>
- optional list of <subgroup> components represents the hierarchy of subgroups in the <group>
- optional <role> component indicates particular position of the user; scoped to the rightmost (sub)group
- <group-authority> indicates the authoritative source for the group membership and role information



Check-in Community AAI service options

Multi-tenant service

- All the standard Check-in authentication options
- Community management using COmanage or Perun
- Basic customisation of user-facing interfaces (e.g. community-specific themes for enrolment flows, group management)
- Basic customisation of AAI proxy behavior

Dedicated service (individual components or AAI service as a whole)

- Customisation of user-facing interfaces: WAYF, enrolment, group membership UI
- Customisation of AAI proxy behaviour (e.g. attribute aggregation rules, service entitlements/capabilities)
- Integration with the EOSC-hub AAI e-Infrastructure SP Proxies for accessing EOSC services and resources

Kubernetes



- Kubernetes is an open-source platform for automating deployment, scaling, and operations of application containers across clusters of hosts, providing container-centric infrastructure.
- Some concepts:
 - Pod: group of one or more containers, shared storage and options to run the containers
 - Deployment maintains the desired count of Pods all the time
 - Service: logical set of Pods and a policy by which to access them.
 - Exposed to the exterior of the Kubernetes cluster via mapping of ports and or Load Balancing
 - Job: A job creates one or more pods and ensures that a specified number of them successfully terminate.



apiVersion: apps/v1 kind: Deployment metadata: name: frontend

spec:
 selector:
 matchLabels:

app: guestbook tier: frontend replicas: 3 template:

> metadata: labels: app: guestbook tier: frontend

spec: containers:

> name: php-redis image: gcr.io/google-samples/gb-frontend:v4 resources: requests:

cpu: 100m memory: 100Mi

env:

- name: GET_HOSTS_FROM value: dns

ports:

- containerPort: 80

apiVersion: v1 kind: Service metadata: name: frontend labels: app: guestbook tier: frontend spec: # comment or delete the following line if you want to use a LoadBalancer type: NodePort ports: - port: 80 selector: app: guestbook tier: frontend apiVersion: extensions/v1beta1 kind: Ingress metadata: name: frontend spec: rules: - host: frontend.test.fedcloud.eu http: paths: - backend: serviceName: frontend servicePort: 80

Example



EGI Cloud Container Kubernetes

- Provides Kubernetes v1.10
- Major differences with other offerings:
 - LoadBalancer ServiceType:
 - A NGINX ingress configured by default ready to be used offering similar functionality
 - Expandable with auto-configuration of Let's Encrypt certificates
 - Dynamic provision of volumes for PersistentVolumeClaims
 - No block-storage directly available
 - NFS-based volumes available instead

A note on AAI



- EGI Cloud Compute currently relies on legacy X.509 + VOMS proxies for access to resources
 - For users without certificates:
 - PUSP with user-personalised proxies from robot certificate
 - RCAuth Online CA to obtain personal proxies from EGI Check-in identities
- Now rolling-out production providers with native OpenID Connect support
 - 2 sites now available, more coming
 - No need for certificates at all!