ISTI: migrazione dei servizi come occasione per l'introduzione di automazione e integrazione

Andrea Dell'Amico <andrea.dellamico@isti.cnr.it>

ISTI-CNR Laboratorio InfraScience

Servizio Infrastruttura Informatica ISTI e Supporto ai Servizi (S2I2S)

Responsabile: Franca Debole

Componenti:

- Tommaso Piccioli
- Andrea Dell'Amico

Philosophical choices

• Free software everywhere

Architectural choices

SMTP: Load balancer vs DNS

- Load balancer: single endpoint that distributes the requests to N backends
- DNS: more than one MX record, or more than one IP address associated to a hostname

Why a load balancer:

- Backend servers can be added or removed transparently to the user
- Email clients cannot be easily configured with more than one SMTP server for one email address
- The web services can be proxied by a load balancer without changes to the application, when a single instance is involved

Load balancers architecture

- 2 Virtual Machines
- 1 floating IP
- Services running on every VM:
 - HAPROXY
 - Keepalived, for HA and floating IP management



Email system: authentication (FreeIPA)



- Incoming SMTP: check of the recipient's email address
- SMTP delivery: find the recipient's username
- POP/IMAP, webmail: user authentication
- Outgoing SMTP: user authentication, authorize the sender's email address

Incoming SMTP



- Two servers behind the load balancers
- Before the delivery
 - RBL check (SpamHaus ZEN)
 - DBL check (SpamHaus)
 - Antivirus check
 - Antispam check
- Different route for the mailing lists
- Delivery via LMTP

Antispam and antivirus

Two VMs, each running both the antivirus and the antispam service

- The antivirus rejects the emails immediately
- Every antispam rule assign points (positive or negative).
 Over 5 (default) an email is marked as SPAM



Outgoing SMTP service



- Services and physical users use two different SMTP servers
- Both servers check the outgoing emails for viruses
- The SMTP server used by the physical users checks the sender's email address
- The delivery rules will diverge in future, between services and users



SMTP: Reputation policies

• SPF enabled and enforced: only the IP address of our SMTP servers are allowed by the policy, with one exception

In the near future

- DKIM
- DMARC
- MTA-STS

IMAP and POP service



- Three *director* servers behind the load balancers
- Four POP/IMAP servers
- The NFS server exports the same volume to all the POP/IMAP servers (SPoF)



Filters, antispam, vacation, forward settings are accessible from inside the webmail interface. Their use is documented at https://mediawiki-s2i2s.isti.cnr.it/

> Server Autern Certifi PKI DOCL Eduro Regist Wiki ir deftag delTin

DOC /

Impostazioni		Azioni				
幸 Preferenze	> main					
Cartelle	Flagged spam					
🖬 Identità	T denyhosts notifications					
Risposte	T root at ISTI					
Informazioni utente	T nostmaster at isti					
	 dom/hosto of recearch in 	feasteraturas				
File	V nanine					
	T nagios					
er inotro						
O Spam	EGI fedcloud notification	15				
P Chiavi PGP	T monit at ICM					
	T d4s jenkins builds					
	T d4s jenkins releases					
	T ckan catalogue notificat	ions				
	VRE user removal					
	T OpenAIRE users VRE					
	T Sindacati					
	RDA-SCID-WG					
	T HydePark					
	TEGI press	andrea.dellamico@isti.cnr.it	;	k to ≞ Ø		
	Formazione GA	➤ Infrastructure		Q. Ceros		
	Notifiche wiki s	D CA		Diego Latella Lur		
	Git DNet	denyhosts		IHYDEPARK-AREAlRobustness and Explainability of Artificial Intelligence - From technical the Fosca Giannotti Luri		
	T Hurlemark Area	it-reti		[HYDEPARK-AREA]Fwd: RACF; osservazioni del MIUR e autonomia del CNR: la battaglia finale [accention]		
		La letsencrypt		Introce orannom Introce Introce orannom Introce Introce orannom Introce Introce orannom Introce Introce orannom Introce		
		monitoring-notifications	8	Diego Latella Lur • IHYDEPARKI Robustness and Explainability of Artificial Intelligence - From technical to policy		
	EDOROAM-TEC	D postmaster	13	Diego.Latella Gio		
		D progetto-cloud-federata		[HYDEPARK-AREA] Biennale Tecnologia - Politecnico di Torino Diego Latella Gio		
				[HYDEPARK] Biennale Tecnologia - Politecnico di Torino		
		🗅 tasks		IHYDEPARK) Fwd: Cercasi dottorando		
		✓ ☐ maling-lists		Diego.Latella Mes (HYDEPARK) Fwd: Invitation to a Pugwash Netherlands Webinar on Al, Drones and Cyberwarl		
		Commercials		Diego Latella 2020-11-05		
		C docker		 [HYDEPARK] Robot soldiers could make up quarter of British army by 2030s¹ - The Guardian Diego.Latella 2020-11-05 		
		hydepark		[HYDEPARK] Fault in NHS Covid app meant thousands at risk did not quarantine - The Guardi Direct staffs		
		D open-infrastructure		[HYDEPARK-AREA] New SIPRI report: Responsible Military Use of Artificial Intelligence: Can t		
		🗅 overleaf		Diego.Latella 2020-11-04		
		✓ □ nmis		Cristina Muntean 2020-11-04		
		D labrimis		Introdemanks Gali for papers Mickos 2021 gi EGH 2021 Diego Latella 2020-11-04		
		Posta inviata		[HYDEPARK] Fwd: [Grin-discuss] giole e soprattutto dolori della trasformazione digitale - il mi Diano stella 2020-11-0		
		 ✓ □ progetti 		[HYDEPARK] [FROM RISKS] Elon Musk's SpaceX says it will make its own laws on Mars (ind		
		auth_federation		Diego Latella 2020-10-23 • [HYDEPARK] Il Presidente dell'Accademia dei Lincei dice: "Servono provvedimenti drastici adi		
		✓ □ cloud		Diego Latella 2020-10-23		
		Cineca		Intructiventy Unipato al articoli al ottobre della Communications of the ACM Shria Borracchi 2020-10-15		
		E EOSC-ICDI		[HYDEPARK-AREA] divulgazione Dieno Latella 2000 10 00		
		task-force-fpc-icdi		[HYDEPARK] More on Cambridge Analytica (UK Channel 4) - From: [RISKS] Risks Digest 32.30		
		C cnr-outreach		Diego Latella 2020-10-00 [HYDEPARK-AREA] More on Cambridge Analytica (UK Channel 4) - From: [RISKS] Ricks Dieve		
		➤ □ d4science		Diego.Latella 2020-10-01		
		C aginfra		 [HYDEPARK] Re: [Ricercatori] Re: [Tecnologi] Re: Re: Pwd: Accesso negato al webinar 'IL COD straccia 2020-10-01 		
		ariadne basho-riakos		[Tecnici] Re: [Ricercatori] [Tecnologi] Re: Re: Fwd: Accesso negato al webinar 'IL CODICE DI C [Inco Davasilante		
		D bluecloud		Introduction of the second secon		
		🗅 déscience		Luca Pappalardo 2020-10-01 ISTAFF-ISTI Socinfo2020: a conference organized by ISTI-CNR on 6-9 October 20200		
				percent of a contraction of a generation of a contract of		

Anispam I legisme I legisme I legi			
Image partial Image partial partex partex partial partial partial partex partin parti	Antispam		
I Repart in a property of any difference of a	Indice (nascondi)		
a transmission of the second secon	1 Riepliogo del funzionamento generale del servizio antispar 2 identificare un managenia di parte aletterale como CDAM	n	
 a Plongs span (and) b Plong	 Identificare un messaggio di posta elettronica come Srivini Interfaccia del sistema antispam e opzioni a disposizione di 	lell'utente	
 A production general (general legeneral (general legeneral general ge	3.1 Settings: Spam (Junk)		
A space of the	3.2 Impostazioni generali (general settings) 3.3 Test snam su Internet (Internet based Junk tests)		
2 3 Registe underge (uddees need) Experiments on a mensage in de laverzion antispan • use espis de la funzionamento generale della verzion antispan • use espis de la funzionamento generale della verzion antispan • use espis de la funzionamento de la verzion de la funziona de laverzion de la funziona d	3.4 Impostazione filtri bayesiani (Bayes settings)		
Religion del funzionamento generale del servicio antispari	3.5 Regole su indirizzi (Address rules)		
 I alra andragen intrabite con un encasation d prateging determined and use area de major, de conse agraveradore a	Riepilogo del funzionamento generale (del servizio antispam	
 • Lan issage in acate it one software i privace i and i thin i duda it, are user i were it is SPAM i reacego a submittamente meta actigo to gont. • Landia contantia contantia contantia contantia contantia submitta i servato i acontatia submitta i servato i acontatia submitta i dudi aconta submi	 Il sistema antispam funziona con un meccanismo di pu viene respinto direttamente. 	nteggi determinati da una serie di regole, che sono aggiornate quotidianamente. Quando il p	punteggio supera 5 il messaggio è marcato come spam vengono aggiunti header per dichiararto tale, e il subject del messaggio è modificato con l'aggiunta del testo [SPAM]. Se il punteggio supera la soglia di 15, il
• I service de contratio de contratio de contratio de contration por investe stiller a legisla de service Stiller de legisla de contration de services. • I service de contration de contration de contration de contration de services. • I service de difference and contration de contration de services. • I service de difference and contration de services. • I service de difference and contration de services. • I service de difference and contration de services. • I service de difference and contration de services. • I service de difference and contration de distances. • I service de difference and contration de services. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de difference and contration de distances. • I service de distances and contration de distances. • I service de distances and contration de distances. • I service de distances and contration de distances. • I service de distances and contration de distances. • I service de distances and contration de distances. • I service de distances and contration de distances and contration. • I service de di	Tutti i messaggi marcati come SPAM vengono intercett	tati dai filtri di default, sul server IMAP, e spostati automaticamente nella cartella SPAM. I me	issaggi presenti in SPAM vengono automaticamente rimossi dopo 90 giorni.
Total products of altifuing under solubility and products of altifuing and under solubility and under solubilit	 Il servizio è contattato dai soli server SMTP di ingresso I dattanti termini sul funzionemento del senvizio sono rieno 	, e non viene attivato per i messaggi inviati dai nostri server SMTP di uscita (sia utente che s mitili en luizi di europorto, che richierte autenticazione: Antienem, e. Anticiper0.	servizi).
NOTA, 1: a clasmera accounting to montane 1 genergio si data	NOTA: Le preferenze dell'antispam sono associate all'indi	rizzo email configurato come principale nelle preferenze del proprio profilo webmail. Se ques	sto non coincide con l'indirizzo usato normalmente, quatunque personalizzazione del sistema antispam risulterà inefficace.
NOTA 2 rome easies un figu de permeta altudente d'adativare i sevoito antiquem per se stesso. Un intuitate equivalente può essere ottenute aggiungendo come whitelis Accente mai destrute a e-perper indicade distance / equiper i	NOTA_1: è caldamente raccomandato non modificare il pi	unteggio di default.	
Identificare un messaggi di posta deltronica come SPAM Testema antigum on è in prace di dentificare serpe kull messaggi di SPAN. Nei caso in usi un usi usi un	NOTA_2: non esiste un flag che permetta all'utente di disa	ttivare il servizio antispam per se stesso. Un risultato equivalente può essere ottenuto aggiu	ingendo come whitelist Accetta mail destinate a «proprio_indrizzo@isti.cnr.it» (redi il paragrafo Regole su indrizzi (Address rules)).
Is stema antispan on e n grade d identificare serve kull message d SPMA. Net cace in ou un message d SPMA rol is active distribution come tais, possible addetted in a province ou van wohal e mercando come Speen (Lake por childran possible come tais) and the serve addet ou van message d SPMA. Net cace in ou un message d SPMA rol is active for the serve for the serv	Identificare un messaggio di posta elett	Ironica come SPAM	
Image: A spin of the sp	Il sistema antispam non è in grado di identificare sempre t	utti i messaggi di SPAM. Nel caso in cui un messaggio di SPAM non sia stato identificato con	me tale, è possibile addestrare il sistema accedendo alla propria posta via webmail e marcando come Spam (Junk per chi usa l'Interfaccia in inglese) il messaggio selezionato:
Q. Onc. Q. Onc. Q. Onc. Q. Onc. Q. Onc. December 2002/ Status (D. F. 147/522 Status (D. Check-in (ALA)), "December 2004/" Status (D. Check-in (ALA))," December 2004/" Status (D. Check-in (DLA))," December 2004/" Status (DLA)," December 2004/" Status (DLA))," December 2004/" Status (DLA))," December 2004/" Status (DLA)," December 2004/" Status (DLA))," December 2004/" Status (DLA))," December 2004/" December 2004/" Status (DLA))," December 2004/" Statu		Deletiona Argomenti Optioni Appli	maa Rapandi Rapandi Li, haday Bhinas Activity Ramas Activity Rama Activity Ramas
Porte informance en la porte informa de l		Q. Ceroa	GGUS-Ticket-ID: #147582 "SOLVED" 'Check-in (AAI)" 'D4Science.org would like to
Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente Interfaccia del sistema antispame e opzioni a disposizione dell'utente		Berviz di infrastruttura (infrastructure servi	Upp List Become a OpenID Connect Service Provider 2
Australizzatione Not and the special spe		support Columpidations org Deficience Description - Task #195131 Sever	We1137 Bringh
Desta adore è pis efficare se il sistema aff lis bayesiari è attivo, compreso fapperdimento adoradora di l'interno del servicio di servicio di servicio de servicio di servicio de servicio ad servicio a personalizzabile da parto degli unite france se il sistema antispame e opzioni a disposizione dell'utente Teatma antispam di avricio di parto degli unite france del servicio di servicio a servicio a personalizzabile da parto degli unite france del servicio di servicio a di rotorico de servicio a personalizzabile da parto degli unite france del servicio di servicio a di rotorico de servicio a personalizzabile da parto degli unite france del servicio di vedenta professore antigamente Teatma esta di los dell'utente		support (chat@discience.org	s constant. Multish Pear user,
• Guide Traver on CDUE Traver o		 [gCube - Feature #19512] DataMiner - Support Invited existing out and a second s	anthe Ren
Quarta actione à più effaces se il astema al filti bayestani è attivo, compreso fappenedmento autonatico. Vedi lepotazione filti bayestani Interfaccia del sistema antispam e opzioni a disposizione dell'utente I astema antispam dei servicio di posta elettorica è personalizzable da parte degi utenti tramite un menu dedicato all'interno dei servicio di webmait: preference antispam # Settings: Spam (utent)		GGUS-Ticket-ID: #147582 "SOLVED" "Check-	HOADYTE. Floor read this email corefully as your input may be required.
Interfaccia del sistema antispam e opzioni a disposizione dell'utente I sistema antispam del servico d posta deterorica è personalizzable da parte dogi usent trante un menu dedicato all'interno del servico di vebmai: preferenze antispam.@ Settings: Spam (Junk)	Questa azione è più efficace se il sistema di fitri bayesiani	è attivo, compreso l'apprendimento automatico. Vedi Impostazione filtri bayesiani	
I sistema antispam del servizio di posta detettorica è personalizzabile da parte dogi utenti trantite un menu dedicato all'interno del servizio di webmait preferenze antispam //	Interfaccia del sistema antispam e opzi	oni a disposizione dell'utente	
Settings: Spam (Junk)	Il sistema antispam del servizio di posta elettronica è pers	onalizzabile da parte degli utenti tramite un menu dedicato all'interno del servizio di webmail	: proferenze antispam @
Settings: Spain (Junk)	Cattinger Course (Junit)		
	Settings: Spam (Junk)		
	Impostazioni		
mpestation	序 幸 Preferenze	💥 Impostazioni generali	Ooxiaal winalaali
Importation Importation // # Information operated Antipolation operated	Nuovo mes.	Lest spam su internet	Un asterisco (*) può essere usato come carattere 'joliy' per aumentare la flessibilità della regola. Ad esempio: *(ikdominio.com o *.dominio.com.
Impostation Impostation Impostation Polentiza Polentiza Option joinfoigail Impostation © Ontele Extension (pipe serve unato come castettere join) per serve unato come castettere join) per serve unato come castettere join	E-Mail Ell Identità	Impostazione filtri Bayesiani	Consent DA (From:) • EMiai Agebon
Impositation Impositation Option principali 2 Preference X Impositation operands Option principali C Printe X Impositation operands Databased come catalities july per aumentate is fiesabilità della majola. Ad esemple "gidomitia.com o "dominic.com. C Printe Impositation of Impositation Databased come catalities july per aumentate is fiesabilità della majola. Ad esemple "gidomitia.com o "dominic.com. C Printe Impositation of Impositation Databased come catalities july per aumentate is fiesabilità della majola. Ad esemple "gidomitia.com o "dominic.com.		Regole su indirizzi	1 Import addresses 🖀 Car
Importation Importation C rest Production Strepsizationing regarding Option principall C rest Strepsizationing regarding Strepsizationing regarding Option principall C rest Strepsizationing regarding Strepsizationing regarding Option principall G rest Strepsizationing regarding Strepsizationing regarding Strepsizationing regarding G rest Strepsizationing regarding Strepsizationing regarding Strepsizationing regarding G rest Strepsizationing regarding Strepsizationing regarding Strepsizationing regarding	🕰 🗭 Risposte		
Importation Importation Importation Importation Option principal Importation Importation (principal) Option (principal) Importation Importation (principal) Importation (principal) Importation Importation (principal) Importation (principal) Importation Importation (principal) Importation (principal) Importation (principal) Importation Importation (principal) Importation (principal) Importation (principal) Importation (principal) Importation Importation (principal) Importation (principal) Importation (principal) Importation (principal) Import address Import address Import address Import address Import address	Contarii Contarii Contarii		Reppia E-Mail J
Importation Importation Importation Importation Opdot principal Importation Importation (principal) Importation (principal) Importation	Contuition Contui		Regala E-Mail Å Nieg DA (Form) Tgiblarteon de
Importance Importa	Risposte Contatil Contatil Contatil Provide Informazioni utente Provide Ufficio Fuent ufficio Indima	Wood Pice This de messaggie in anne.	Region E-Mail I Nega DA (From) *@Batantion.de
Image:	Contract P Reporte Contract P First Proportizion V First V First V First Intolficio V Fund Histio	Notifice TPP dat montages in price.	Regula E-doil I Nega DA (From) *QBazamion.de Nega DA (From) *QBazamion.de

ega DA (From:) rdcpisa@gmail.com

前

Operations

- Everything over TLS (not limited to https)
 - Letsencrypt is being used not only for web certificates
 - Certificates renewals are automatic
- Firewall rules on every VM

(or: *is it zero trust?*):

- Minimal set of open ports
- Services that are not public are limited to the allowed clients

- No direct root access
- Use of the VPN is mandatory

Problem

A lot of very old clients still in use → we cannot remove support for tls < 1.2 yet

Task #28

Status:

Priority

Assignee:

Category:

Description

Attivazione di un nuovo sistema di posta elettronica per l'ISTI Added by Andrea Dell'Amico over 1 year ago. Updated 24 days ago.

Migrazione servizi ex Gennai

Questo vuole essere il task padre di tutte le attività, che comprendono parecchi servizi. Task dettagliati verranno aperti in seguito

In Progress

High

s2i2s

Operations: everything is a ticket, at https://redmine-s2i2s.isti.cnr.it

Una descrizione di come dovrebbe essere strutturata tutta l'architettura, compresa anche la posta elettronica, è definita in https://c Una copia PDF del documento è disponibile su nextcloud: https://nextcloud-s2i2s.isti.cnr.it/s/SA9rExkfLHoPw6K	locs.google.com/document/d/1kcCn_jG	Gdi6uhfGxRwHqWzlyxFDK4qIIsqefJ7	pEk2G8/edit	?usp=sharing			
Subtasks						Add	
Task #147: Installare e configurare tre server che ospiteranno il servizio di posta, in attesa dell'infrastruttura definitiva	Closed	s2i2s					
> Service #37: VM sulla quale installare imapsync e una interfaccia web che collezioni i dati di accesso degli utenti	Closed	s2i2s					
> Task #153: Configurare KVM sui due server di calcolo del piano B	Closed	s2i2s					
> Task #154: Configurare lo storage server del piano B	Closed	s2i2s					
> Task #196: Installare due VM che funzioneranno da load balancer per i server pop/imap e per webmail	Closed	s2i2s					
> Task #197: Installare le due VM che funzioneranno da server pop/imap	Closed	s2i2s					
> Task #198: Configurare NFS tra lo storage server e le macchine del servizio pop/imap	Closed	s2i2s					
> Task #199: Installare e configurare due VM per postgresgi	Closed	s2i2s					5
> Task #200: Installare e configurare due macchine sulle quali installare il servizio webmail	Closed	s2i2s					F
> Task #203: VM col servizio SMTP, che distribuisca a pop/imap	Closed	s2i2s					ł
> Task #207: Modificare il record SPF per il dominio isti.cnr.it	Closed	s2i2s					
> Task #231: Servono 6 VM da usare come load balancer per i server SMTP in uscita e in ingresso	Closed	s2i2s					
> Task #232: Due VM per gestire il servizio SMTP in uscita da parte dei client	Closed	s2i2s					
> Task #233: Due VM per gestire il traffico SMTP in uscita generato da servizi	Closed	s2i2s					
> Task #234: Due VM per il traffico SMTP in ingresso	Closed	s2i2s					
> Task-#244: 3 VM con dovecot configurato in modalità 'director'	Closed	s2i2s					
> Task #248: Chiedere allo IIT di aprire il firewall ai nostri servizi di posta	Closed	s2i2s					
> Task #268: Aggiungere due VM. CentOS based, sulle guali installare i servizi antivirus	Closed	s2i2s					
> Task #303: SMTP per gestire il traffico in uscita dai nodi dovecot	Closed	s2i2s					
Incident #304: I server SMTP per il delivery non hanno ricevuto posta per alcune ore	Closed	s2i2s					
Task #254: DOC:Documentare la configurazione necessaria per usare il nuovo server iman.	Closed	\$2125					
Task #255: DOC:Documentare l'uso dei filtri di nosta sul server iman (via webmail)	Closed	s2i2s					
Task #263: Lista di questioni aperte relative al 'vecchio' sistema di posta	Closed	s2i2s					
Task #279: DOC:Disegnare l'architettura del nuovo sistema di posta	Closed	s2i2s					
Task #271: DOC:Documentare le caratteristiche tecniche del sistema di posta	New	s2i2s					
Tack #285: Utente ner i test di varation e forward	Closed	\$2125					
Task #294; webmail: aquinnere la possibilità di cambiare i temi	Closed	\$2125					
Task #295: Record MX per testare i server SMTP in ingresso	Closed	s2i2s					
Task #296: Interfactia che permetta adii utenti di ossirie la configurazione dell'antispam	Closed	\$2125					
Task #575: Modificare il ruolo ansible di roundcube per la gestione del blugin sauserspref	Closed	Andrea Dell'Amico					
> Task #605: webmail: pyzor attivo di default	Closed	s2i2s					
Task #306: Gestione litenti di MalhovManager	In Progress	\$2125					
Task #211: Alias deali utenti di nosta	Closed	Erança Debole					
> Tack #AR8: Migratione denti alias su Mailman3	Closed	Erança Debole	# *	Project	Tracker	Status	
Tidsk # 5000 Fingligatione degle direct and an inflation Tidsk # 5000 Fingligatione degle direct and inflation	Closed	e2i2e	993	Possibili evoluzioni Possibili evoluzioni	Feature	New	
Sociality Engineering and intenti di posta Task 4214 - Engineering deni utenti di posta	Closed	c2i2c	774	Possibili evoluzioni	Service	New	
) Took #127 100 Retione degli utenti che spedicono e laggono mail e sono legati ai servizi, su freeina	Closed	c2i2c	684	Possibili evoluzioni	Feature	New	
 Task #307: Gestione degli denti die goziatione eleggioni mare sono regul di servizi, su recepti 	Feedback	c2i2c	635	Possibili evoluzioni	Service	New	
Task #300; Utenti di servizi / DD	Closed	Vittorio Romano	609	Possibili evoluzioni	Feature	New	
	Closed	Marco Tampucci	549	Possibili evoluzioni Possibili evoluzioni	Service	New	
> Task #240: Utenti di servizi.DTD	Closed	Eprico Eantini	313	Possibili evoluzioni	Service	New	
Adde #900, Occident and Park Adde #900, Occident and Park Adde #900, Occident and Park	Closed	e2i2e	288	Possibili evoluzioni	Feature	New	
Tak Fore Gestione of the disconstruction of the second sec	Closed	SZIZS	287	Possibili evoluzioni	Feature	New	
 Task #011. Utenti di Servizi MIC Task #204: Utenti di Servizi MIC 	Closed	Dapiele Pellegrini	243	Possibili evoluzioni	Service	New	
> Task #35%. Utenti di cervizi-inita	Closed	Alassandro Coco	240	Possibili evoluzioni	Service	New	
	Closed	Antonello Calabrò	239	Possibili evoluzioni	Feature	New	
Tack #202: Itenti di centizi-EMT	Closed	Gianluca Treatann	206	Possibili evoluzioni	Feature	New	
Tack #3097. Otenti di servizi-SB Tack #3099. Utenti di servizi-SB	Closed	Caterina D'Angolo	205	Possibili evoluzioni	Feature	New	
 Task #300. Utanti di servizi SM 	Closed	Cievanni Lambard	(1. 1.B.(1.F.)				
Task #333, Utenti di servizi SEDI Task #400, Utenti di servizi SEDI	Closed	Giovanni Lombard	(1-17/17)	_			
Task #401: Utasti di servizi-XC Task #401: Utasti di servizi-XC	Closed	Euclario Anseimo					
Tack #402: Utenti di cenvizi-WN	Eeedback	Francesco Potorti					
· IUSK # TV2. OCOTO OF SCI 121 TWIN	recubaux	riancesco Potorti					

Clocod

Start date:

Due date:

Estimated time:

% Done:

11 Feb 2020

10 Jun 2020

20%

(Total: 0:00 h)

 Task	77	227	304
 Service	5	15	20
 Feature	21	50	71
 Hardware resource	3	6	9
 Bug	9	36	45
 Incident	2	52	54
 Documentation	4	8	12

ject	Tracker	Status	Priority	Subject	Assignee	Updated	Due date	
voluzioni	Feature	New	Normal	SIEM: attivare una infrastruttura di logging e report compatibile SIEM	s2i2s	02 Nov 2020 04:37 PM		
voluzioni	Feature	New	Normal	Plugin nextcloud per la webmail	s2i2s	05 Oct 2020 08:12 PM		
voluzioni	Service	New	Normal	Autodiscovery per la configurazione della posta	s2i2s	24 Jun 2020 01:07 PM		
voluzioni	Feature	New	Normal	Attivare DNSSEC sulle nostre zone	s2i2s	20 May 2020 02:39 PM		
voluzioni	Service	New	Normal	Servizio che permetta di gestire newsletter	s2i2s	20 Apr 2020 02:11 PM		
voluzioni	Feature	New	Normal	Recupero password self service su freeipa	s2i2s	15 Apr 2020 08:25 PM		
voluzioni	Service	New	Normal	Zulip come chat collaborativa	s2i2s	16 Mar 2020 08:24 PM		
voluzioni	Feature	New	Normal	Form per la richiesta di registrazione dei domini	s2i2s	12 Feb 2020 10:36 AM		
voluzioni	Service	New	Normal	Look dell'interfaccia web dell'autenticazione dell'IdP	s2i2s	21 Feb 2020 11:55 AM		
voluzioni	Feature	New	Normal	Soluzione per il Disaster recovery	s2i2s	27 Dec 2019 05:01 PM		
voluzioni	Feature	New	Normal	Sistema di backup con cifratura	s2i2s	27 Dec 2019 06:42 PM		
voluzioni	Service	New	Normal	Ricerca server side per le email	s2i2s	29 Nov 2019 07:55 PM		
voluzioni	Service	New	Normal	Mailbox sull'object storage	s2i2s	29 Nov 2019 07:47 PM		
voluzioni	Service	New	Normal	Notifiche push per l'email	s2i2s	29 Nov 2019 07:46 PM		
voluzioni	Feature	New	Normal	Mailbox cifrate sul server imap	s2i2s	29 Nov 2019 07:44 PM		
voluzioni	Feature	New	Normal	Valutare l'introduzione di DNS over HTTPS	s2i2s	29 Nov 2019 07:44 PM		
voluzioni	Feature	New	Normal	Valutare 'LetsMapYourNetwork'	s2i2s	29 Nov 2019 07:44 PM		

October 15, 2021

> Tack #414: Utenti di servizi-HIIS

Marco Manca

Operations: monitoring

What we have (Zabbix)

- Hardware status
 - Disk space
 - Free memory
 - Load average
 - Disk I/O activity
 - Is the server alive?

What we are going to have

- Observability (Prometheus + Grafana)
- Services status
- Services behaviour
- Status dashboard
- Incident history

urrent status			
Sit Operations (?)	٢	API Requests ⑦ Normal	0
Nebhooks 🕐	Ø	Issues ⑦ Normal	Ø
Pull Requests ⑦	0	GitHub Actions ⑦ Normal	Ø
SitHub Packages 💿	۲	GitHub Pages ⑦	Ø

Deployment: everything is automated (mostly) *010

Ansible is the provisioning tool used to configure all the servers and all the services.

- All the servers share a basic configuration set (language, ssh access, timezone, firewall, dns resolver, NTP, ...)
- No manual editing of configuration files
- A new instance of a server ۲ can be ready in a matter of minutes

ansible-role-node-js Installs node-js from nodesource.com. And, optionally, yarn.	★ 0 ¥ 0
Updated 2 months ago	ansible-role-docker-registry 🔒
ansible-role-elasticsearch Ansible role that installs the free compc Updated 2 months ago	Role that installs a Docker registry Updated 1 week ago
ansible-role-letsencrypt-; Ansible role that manages x509 certific Updated 3 months ago	ansible-roles Ansible roles used by our playbooks Updated 2 weeks ago
ansible-role-thredds Role that installs the THREDDS Data St Updated 3 months ago	ansible-role-basic-system-setup Basic setup of a VM
ansible-role-python3-env Role that installs python3 and eventuall Updated 3 months ago	Updated 2 weeks ago
ansible-role-openjdk Role that installs openjdk. The Zulu dist repository) Updated 3 months ago	ansible-role-squid Installs and configure a basic squid caching proxy serv Updated 2 weeks ago
ansible-role-prometheus- Installs the prometheus node exporter. Updated 3 months ago	ansible-role-nginx Role that installs and configures nginx Updated 2 weeks ago
ansible-role-prometheus Role that installs the prometheus serve Updated 4 months ago	ansible-role-epas-client-timbrature Ruolo che installa il container del cient timbrature.
ansible-role-dovecot Role that installs the dovecot IMAP sen Updated 4 months ago	Updated 2 weeks ago
anallela nala farra larratan	ansible-role-epas
An Store - Tote - JaVa - Keystor Manages a java keystore Updated 4 months ago	Role that installs ePAS as a docker swarm stack Updated 3 weeks ago
ansible-role-simplesaml This ansible role installs simplesaml. Updated 4 months ago	≪ First ← Previous 1

ansible-role-postfix Role that installs postfix Updated 3 weeks ago ansible-role-keycloak Role that installs the Keycloak IdM, ansible-role-docker-swarm Creates a docker swarm cluster. With portainer and haproxy ansible-role-shinyproxy Installs and configure shinyproxy. Standalone or as a containe

ansible-role-memcached Installs and configures the memcache service

★0¥0

Updated 3 weeks ago

ansible-role-redmin

Role that installs redmin

ansible-role-linux-firewall Configure a set of firewall rules on a linux system

ansible-role-php-fpm Ansible role that installs php-for Updated 1 week ago

ansible-role-docker Installs docker or a docker swarm clust

ansible-role-haproxy

Role that installs haprox

ansible-role-tomcat-multiple-instances

Installs multiple instances of the tomcat service using the system packages. Updated 1 week ago

antivirus-servers.yml authoritative dns.yml ca.yml dhcp-server.yml freeipa.yml git-server.yml haproxy-frontend.yml imap-director.yml imap-pop-server.yml imap-sync.yml kvm_hosts.yml mailman.yml mediawiki.yml nextcloud-fileserver.yr postgresql-server.yml powerdns_admin.yml radius.yml redmine.yml resolvers.yml roundcube-webmail.yml san_plan_b.yml simplesaml.yml smtp-servers-in.yml smtp-servers-out.yml squid.yml syslog-collector.yml vm_templates_setup.yml vpn-service.yml

zabbix-monitoring.yml

Andrea Dell'Amico - ICTalk@CNR 2021

Ansible: a brief introduction

Essentials https://docs.ansible.com

- No client/server model. Remote hosts accessed using SSH
- Python based. A basic python setup is required on the target nodes
- Modules can be written in whatever language, but python is easier
- Components: playbooks, tasks, roles, modules, inventory, collections

Ansible concepts: control and managed nodes, inventory, collections, modules, tasks, playbooks

- Ansible runs *playbooks*
- A playbook is a set of tasks, often grouped into roles.
- Tasks use modules. Most modules guarantee idempotency (exceptions: command, shell)
- Playbooks are run on the control node and execute on the managed nodes

Ansible: a brief introduction (2)

A playbook

- A playbook usually lives on the control node
- Its execution is influenced by variables
- Variables can be associated to hosts, host groups, roles, or loaded from files
- Files that define variables, and also files that must be transferred into the managed nodes, can be encrypted

```
- hosts: smtp_avs_servers
serial: 1
roles:
    - { role: pgsql-db-management }
    - { role: ../library/bootstrap-roles/centos-common, when: ansible_distribution_file_variety = "RedHat" }
    - { role: user_services_perms }
    - ../library/roles/ssh-keys
    - clamav
    - spamassassin
```

Ansible: variables

letsencrypt acme install: False letsencrypt_acme_sh_install: '{{ letsencrypt_acme_install }}' letsencrypt_acme_sh_git_install: True etsencrypt_update_acme_distribution: True letsencrypt_acme_sh_git_url: https://github.com/acmesh-official/acme.sh.git letsencrypt_acme_sh_default_ca: 'letsencrypt' letsencrypt_acme_user: acme letsencrypt_acme_sh_user: '{{ letsencrypt_acme_user }}' letsencrypt_acme_user_home: /var/lib/acme .etsencrypt_acme_git_dest_dir: '{{ letsencrypt_acme_user_home }}/acme_sh_dist' etsencrypt_acme_sh_user_home: '{{ letsencrypt_acme_user_home }}' letsencrypt_acme_sh_base_data_dir: '{{ letsencrypt_acme_sh_user_home }}/acme_data' letsencrypt_acme_sh_certs_data_prefix: '{{ letsencrypt_acme_sh_certificates_install_dir }}' letsencrypt_acme_sh_certs_data_path: '{{ letsencrypt_acme_sh_base_data_dir }}/certs/{{ letsencrypt_acme_sh_certs_data_prefix }}' letsencrypt_acme_sh_certificates_install_dir: '{{ ansible_fqdn }}' etsencrypt_acme_sh_certificates_install_base_path: '{{ letsencrypt_acme_sh_user_home }}/live' letsencrypt_acme_sh_certificates_install_path: '{{ letsencrypt_acme_sh_certificates_install_base_path }}/{{ letsencrypt_acme_sh_certificates_install_dir }}' letsencrypt_acme_sh_log_dir: /var/log/acme letsencrypt_acme_sh_install_cron: False letsencrypt_acme_sh_log_enabled: True letsencrypt_acme_sh_auto_upgrade: False letsencrypt_acme_sh_install_options: '--install' etsencrypt_acme_sh_test_request: False letsencrypt_acme_sh_use_syslog: True letsencrypt_acme_sh_syslog_level: 6

Ansible: tasks

```
₩ ansible-tasks.yml ×
42 - import_tasks: acmetool_deb.yml
     when: ansible_distribution_file_variety = "Debian"
39 - import_tasks: acmetool_rh.yml
    when: ansible_distribution_file_variety = "RedHat"
36 - block:
     - name: Create the letsencrypt acme user
       user: name={{ letsencrypt_acme_sh_user }} home={{ letsencrypt_acme_sh_user home }} createhome=no shell=/usr/sbin/nologin system=yes
       tags: [...'letsencrypt', 'letsencrypt_user'..]
     - name: Create the letsencrypt acme home, if it does not exist already. In a separate step because it could be already there.
      file: dest={{ letsencrypt_acme_sh_user_home }} owner={{ letsencrypt_acme_sh_user }} group={{ letsencrypt_acme_sh_user }} state=directory recurse=yes
     - name: Install the acme.sh environment variables file
       template: src=acme_sh_request_env.j2 dest=/etc/default/acme_sh_request_env owner=root group=root mode=0444
       register: acme sh issue
     - name: Install a daily cron job to renew the certificates when needed. It runs as root
       cron:
         name: "Letsencrypt certificate renewal"
         day: '{{ letsencrypt_acme_cron_day_of_month }}'
         hour: '{{ letsencrypt_acme_cron_hour }}'
         minute: '{{ letsencrypt_acme_cron_minute }}'
         job: "/usr/local/bin/acme-sh-cron-script > {{ letsencrypt_acme_sh_log_dir }}/acme-cron.log 2>&1"
       tags: [__'letsencrypt', 'letsencrypt_cron', 'letsencrypt_acme_sh', 'letsencrypt_acme_sh_scripts'...]
     - name: Remove the daily cron job that run as acme user.
       cron:
         name: "Letsencrypt certificate renewal"
         day: '{{ letsencrypt_acme_cron_day_of_month }}'
         hour: '{{ letsencrypt_acme_cron_hour }}'
         minute: '{{ letsencrypt acme cron minute }}'
         job: "/usr/local/bin/acme-sh-cron-script > {{ letsencrypt_acme_sh_log_dir }}/acme-cron.log 2>&1"
         state: absent
       tags: [_'letsencrypt', 'letsencrypt_cron', 'letsencrypt_acme_sh'_]
     become: True
     become_user: '{{ letsencrypt_acme_sh_user }}'
     when: letsencrypt_acme_sh_install | bool
     tags: [..'letsencrypt', 'letsencrypt acme sh'..]
```

Ansible: play run

ansible-playbook --vault-password-file=<LOL>' ca.yml -i inventory/hosts -t letsencrypt

PLAY [certification_authority] ************************************	***************************************
TASK [Gathering Facts] ************************************	**************************************
TASK [postfix-client : Create the acme hooks directory if it Thursday 14 October 2021 20:40:00 +0200 (0:00:03.788) Thursday 14 October 2021 20:40:00 +0200 (0:00:03.788) skipping: [ca.isti.cnr.it]	'does not exist] ************************************
TASK [postfix-client : Install a hook for letsencrypt] ***** Thursday 14 October 2021 20:40:00 +0200 (0:00:00.064) Thursday 14 October 2021 20:40:00 +0200 (0:00:00.064) skipping: [ca.isti.cnr.it]	**************************************
TASK [letsencrypt-acme-sh-client : Install the socat utility Thursday 14 October 2021 20:40:00 +0200 (0:00:00.048) Thursday 14 October 2021 20:40:00 +0200 (0:00:00.048) skipping: [ca.isti.cnr.it]	, needed when using the http protocols to request the certificates] ** 0:00:04.051 ***** 0:00:04.050 *****
TASK [letsencrypt-acme-sh-client : Install the git client if Thursday 14 October 2021 20:40:00 +0200 (0:00:00.044) Thursday 14 October 2021 20:40:00 +0200 (0:00:00.044) skipping: [ca.isti.cnr.it]	we are installing using git] ************************************
TASK [letsencrypt-acme-sh-client : Install the socat utility Thursday 14 October 2021 20:40:00 +0200 (0:00:00.047) Thursday 14 October 2021 20:40:00 +0200 (0:00:00.047) changed: [ca.isti.cnr.it]	, needed when using the http protocols to request the certificates] ** 0:00:04.142 ****** 0:00:04.142 ******
TASK [letsencrypt-acme-sh-client : Install the git client if Thursday 14 October 2021 20:40:07 +0200 (0:00:06.162) Thursday 14 October 2021 20:40:07 +0200 (0:00:06.162) changed: [ca.isti.cnr.it]	<pre>we are installing using git] ************************************</pre>
TASK [letsencrypt-acme-sh-client : Activate the firewalld ru Thursday 14 October 2021 20:40:31 +0200 (0:00:24.652) Thursday 14 October 2021 20:40:31 +0200 (0:00:24.652) changed: [ca.isti.cnr.it] \Rightarrow (item={'domain': 'ca.isti.cnr.it}	le for the http, if we require certificates using the http protocol] 0:00:34.957 ***** 0:00:34.957 ***** t', 'standalone': True})

Evolution of the ISTI infrastructure

The technical buzzwords

- Servers consolidation
- Cloud computing, on premise
 - Infrastructure as a Service (laaS)
 - Platform as a Service (PaaS)
 - Managed Software as a Service (MSaaS)
 - Functions as a Service (FaaS)
 - Object storage
 - Distributed block storage
 - Distributed Posix File system
 - Containers Orchestrator (Kubernetes, Docker Swarm)

What does it even mean?

- Contribute hardware to the infrastructure
- Everything runs in the same infrastructure (when possible)
- Resources available to each laboratory, based on the contributions and the needs
- Federated SSO
- Federated resources, potentially

ISTI Services: next steps

- IAM, to enable SSO between all services
 - 2FA, with both applications (Google authenticator, for ٠ example) and hardware keys: yubikeys, solo keys, feitian, etc (they cost money)

- Security (see the aGID guidelines):
- Logs centralization ٠
- Alerting based on log patterns •
- A SIEM system ٠

name 1019 Possibili evoluzioni Service New Normal Istanza condivisa di Overleaf (sharelatex) negration with the webmail 933 Possibili evoluzioni Feature New Normal SIEM: attivare una infrastruttura di logging e report compatibile SIEM ver general availability 936 Possibili evoluzioni Service New Normal Attivare una infrastruttura di logging e report compatibile SIEM ver general availability 936 Possibili evoluzioni Service New Normal Attivare DNSSEC sulle nostre zone 644 Possibili evoluzioni Feature New Normal Service o sessord self service su freeipa 635 Possibili evoluzioni Service New Normal Service o sessord self service su freeipa 640 Possibili evoluzioni Service New Normal Stetma free (open source) di videoconferenza 637 Possibili evoluzioni Service New Normal Stetma free (open source) di videoconferenza 638 Possibili evoluzioni Service New Normal Slouten eri Insteat at registrazione dell'autenticazione dell'autenticazione dell'autenticazione dell'autenticazione dell'autenticazione dell'	nlyOffice integration	# ~	Project	Tracker	Status	Priority	Subject
993 Possibili evoluzioni Feature New Normal SIEM: attivare una infrastruttura di logging e report compatibile SIEM rver general availability 936 Possibili evoluzioni Feature New Normal Plugin nextcloud per la webmail 0 774 Possibili evoluzioni Feature New Normal Autodiscovery per la configurazione della posta 0 684 Possibili evoluzioni Feature New Normal Stervize on password self service su freeipa 0 905 Possibili evoluzioni Feature New Normal Stervize on password self service su freeipa 0 905 Possibili evoluzioni Service New Normal Stema free (open source) di videoconferenza 0 905 Possibili evoluzioni Service New Normal Soluzione per il Disaster recovery 0 1313 Possibili evoluzioni Service New Normal Sitema di backup con cifratura 0 287 Possibili evoluzioni Feature New Normal Sitema di backup con cifratura 0 287 Possibili evoluzioni Service	raw.io integration	1019	Possibili evoluzioni	Service	New	Normal	Istanza condivisa di Overleaf (sharelatex)
936 Possibili evoluzioni Feature New Normal Plugin nextcloud per la webmail rver general availability 774 Possibili evoluzioni Service New Normal Autodiscovery per la configurazione della posta 684 Possibili evoluzioni Feature New Normal Attivare DNSSEC sulle nostre zone 635 Possibili evoluzioni Feature New Normal Servizio che permetta di gestire newsletter 699 Possibili evoluzioni Service New Normal Recupero password self service su freeipa 549 Possibili evoluzioni Service New Normal Sistema free (open source) di videoconferenza 1313 Possibili evoluzioni Feature New Normal Soluzione per il Disaster recovery 288 Possibili evoluzioni Feature New Normal Soluzione per il Disaster recovery 287 Possibili evoluzioni Service New Normal Normal Notrati backup con cifratura 243 Possibili evoluzioni Service New Normal Normal Notifiche push per il'email 239 Possibi	togration with the webmail	993	Possibili evoluzioni	Feature	New	Normal	SIEM: attivare una infrastruttura di logging e report compatibile SIEM
 774 Possibili evoluzioni Service New Normal Attivare DNSSEC sulle nostre zone 684 Possibili evoluzioni Service New Normal Servizio che permetta di gestire newsletter 635 Possibili evoluzioni Service New Normal Servizio che permetta di gestire newsletter 635 Possibili evoluzioni Service New Normal Secupero password self service su freeipa 639 Possibili evoluzioni Service New Normal Sistema free (open source) di videoconferenza 413 Possibili evoluzioni Service New Normal Look dell'interfaccia web dell'autenticazione dei domini 313 Possibili evoluzioni Service New Normal Soluzione per il Disaster recovery 287 Possibili evoluzioni Service New Normal Neiterca server side per le email 243	itegration with the webmail	936	Possibili evoluzioni	Feature	New	Normal	Plugin nextcloud per la webmail
 684 Possibili evoluzioni Feature New Normal Attivare DNSSEC sulle nostre zone 635 Possibili evoluzioni Service New Normal Servizio che permetta di gestire newsletter 609 Possibili evoluzioni Feature New Normal Recupero password self service su freeipa 549 Possibili evoluzioni Service New Normal Zulip come chat collaborativa 539 Possibili evoluzioni Service New Normal Sistema free (open source) di videoconferenza 413 Possibili evoluzioni Feature New Normal Sistema free (open source) di videoconferenza 413 Possibili evoluzioni Service New Normal Cook dell'interfaccia web dell'autenticazione dei domini 313 Possibili evoluzioni Feature New Normal Soluzione per il Disaster recovery 287 Possibili evoluzioni Feature New Normal Sistema di backup con cifratura 243 Possibili evoluzioni Service New Normal Ricerca server side per le email 240 Possibili evoluzioni Service New Normal Notifiche push per l'email 243 Possibili evoluzioni Service New Normal Mailbox cifrate sul server imap 240 Possibili evoluzioni Service New Normal Mailbox cifrate sul server imap 243 Possibili evoluzioni Service New Normal Mailbox cifrate sul server imap 240 Possibili evoluzioni Service New Normal Mailbox cifrate sul server imap 243 Possibili evoluzioni Feature New Normal Mailbox cifrate sul server imap 243 Possibili evoluzioni Service New Normal Mailbox cifrate sul server imap 243 Possibili evoluzioni Feature New Normal Mailbox cifrate sul server imap 248 Possibili evoluzioni Feature New Normal Mailbox cifrate sul server imap 249 Possibili evoluzioni Feature New Normal Valutare l'introduzione di DNS over HTTPS 205 Possibili evoluzioni Feature New Normal Valutare l'introduzione di DNS over HTTPS 	wor gonoral availability	774	Possibili evoluzioni	Service	New	Normal	Autodiscovery per la configurazione della posta
635Possibili evoluzioniServiceNewNormalServizio che permetta di gestire newsletter609Possibili evoluzioniFeatureNewNormalRecupero password self service su freeipa549Possibili evoluzioniServiceNewNormalZulip come chat collaborativa539Possibili evoluzioniServiceNewNormalSistema free (open source) di videoconferenza413Possibili evoluzioniFeatureNewNormalForm per la richiesta di registrazione dei domini313Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalNotfiche push per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalNotfiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'	ver general availability	684	Possibili evoluzioni	Feature	New	Normal	Attivare DNSSEC sulle nostre zone
609Possibili evoluzioniFeatureNewNormalRecupero password self service su freeipa549Possibili evoluzioniServiceNewNormalZulip come chat collaborativa539Possibili evoluzioniServiceNewNormalSistema free (open source) di videoconferenza413Possibili evoluzioniFeatureNewNormalForm per la richiesta di registrazione dei domini313Possibili evoluzioniServiceNewNormalLook dell'interfaccia web dell'autenticazione deil'IdP288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalRicerca server side per le email243Possibili evoluzioniServiceNewNormalMilbox sull'object storage240Possibili evoluzioniServiceNewNormalMilbox sull'object storage239Possibili evoluzioniServiceNewNormalMilbox sull'object storage240Possibili evoluzioniServiceNewNormalMilbox cifrate sul server imap238Possibili evoluzioniFeatureNewNormalMilbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		635	Possibili evoluzioni	Service	New	Normal	Servizio che permetta di gestire newsletter
549Possibili evoluzioniServiceNewNormalZulip come chat collaborativa539Possibili evoluzioniServiceNewNormalSistema free (open source) di videoconferenza413Possibili evoluzioniFeatureNewNormalForm per la richiesta di registrazione dei domini313Possibili evoluzioniServiceNewNormalLook dell'interfaccia web dell'autenticazione dell'IdP288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage238Possibili evoluzioniServiceNewNormalMailbox cifrate sul server imap240Possibili evoluzioniServiceNewNormalNotifiche push per l'email238Possibili evoluzioniServiceNewNormalMailbox cifrate sul server imap239Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		609	Possibili evoluzioni	Feature	New	Normal	Recupero password self service su freeipa
539Possibili evoluzioniServiceNewNormalSistema free (open source) di videoconferenza413Possibili evoluzioniFeatureNewNormalForm per la richiesta di registrazione dei domini313Possibili evoluzioniServiceNewNormalLook dell'interfaccia web dell'autenticazione dell'IdP288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalMailbox cifrate sul server imap238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		549	Possibili evoluzioni	Service	New	Normal	Zulip come chat collaborativa
413Possibili evoluzioniFeatureNewNormalForm per la richiesta di registrazione dei domini313Possibili evoluzioniServiceNewNormalLook dell'interfaccia web dell'autenticazione dell'IdP288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalMormal238Possibili evoluzioniFeatureNewNormalMailbox sull'object storage239Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap238Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare l'etsMapYourNetwork'		539	Possibili evoluzioni	Service	New	Normal	Sistema free (open source) di videoconferenza
313Possibili evoluzioniServiceNewNormalLook dell'interfaccia web dell'autenticazione dell'IdP288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalMotifiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap238Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS206Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		413	Possibili evoluzioni	Feature	New	Normal	Form per la richiesta di registrazione dei domini
288Possibili evoluzioniFeatureNewNormalSoluzione per il Disaster recovery287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalNotifiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		313	Possibili evoluzioni	Service	New	Normal	Look dell'interfaccia web dell'autenticazione dell'IdP
287Possibili evoluzioniFeatureNewNormalSistema di backup con cifratura243Possibili evoluzioniServiceNewNormalRicerca server side per le email240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalNotifiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		288	Possibili evoluzioni	Feature	New	Normal	Soluzione per il Disaster recovery
 243 Possibili evoluzioni 240 Possibili evoluzioni 240 Possibili evoluzioni 239 Possibili evoluzioni 238 Possibili evoluzioni 238 Possibili evoluzioni 260 Possibili evoluzioni 261 Possibili evoluzioni 261 Possibili evoluzioni 262 Possibili evoluzioni 263 Possibili evoluzioni 264 Possibili evoluzioni 265 Possibili evolu		287	Possibili evoluzioni	Feature	New	Normal	Sistema di backup con cifratura
240Possibili evoluzioniServiceNewNormalMailbox sull'object storage239Possibili evoluzioniServiceNewNormalNotifiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		243	Possibili evoluzioni	Service	New	Normal	Ricerca server side per le email
239Possibili evoluzioniServiceNewNormalNotifiche push per l'email238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		240	Possibili evoluzioni	Service	New	Normal	Mailbox sull'object storage
238Possibili evoluzioniFeatureNewNormalMailbox cifrate sul server imap206Possibili evoluzioniFeatureNewNormalValutare l'introduzione di DNS over HTTPS205Possibili evoluzioniFeatureNewNormalValutare 'LetsMapYourNetwork'		239	Possibili evoluzioni	Service	New	Normal	Notifiche push per l'email
206 Possibili evoluzioni Feature New Normal Valutare l'introduzione di DNS over HTTPS 205 Possibili evoluzioni Feature New Normal Valutare 'LetsMapYourNetwork'		238	Possibili evoluzioni	Feature	New	Normal	Mailbox cifrate sul server imap
205 Possibili evoluzioni Feature New Normal Valutare 'LetsMapYourNetwork'		206	Possibili evoluzioni	Feature	New	Normal	Valutare l'introduzione di DNS over HTTPS
		205	Possibili evoluzioni	Feature	New	Normal	Valutare 'LetsMapYourNetwork'

- Nextcloud general availability, and
 - 0
 - D
 - In
- Git ser



Infrastructure: next steps

- Fix the wiring between switches and servers
- Start the OpenStack installation (hyperconverged)
- Test the functionalities
- Test at least one live upgrade of the OpenStack distribution
- Start migrating the ISTI and InfraScience (D4Science) services



Hyperconverged: each server is used for both computing and distributed storage



Una infrastruttura complessa: perché tanto odio?*

(* cit. https://fr.wikipedia.org/wiki/Édika)

L'impegno per la realizzazione di una infrastruttura così complessa è giustificato dalla necessità di fornire servizi sofisticati

Servizi specifici per l'istituto

- Posta elettronica
- DNS
- Autenticazione
- Supporto agli utenti
- Wiki
- Git
- Cloud storage (nextcloud)
- (eccetera)

Supporto alla ricerca (D4Science, OpenAIRE): VRE, Virtual Research Environments

- VRE (Virtual Research Environment): storage, messaggistica, social
- Autenticazione federata (soggetta all'accettazione di Terms of Use)
- Servizi gestiti, disponibili ai ricercatori (JupyterHub, Rstudio, Shinyproxy, OverLeaf, catalogo CKAN-based, Geoserver, Geonetwork, Hadoop...)
- Esecuzione di esperimenti con workflow FAIR (Analytics Engine, prossimamente container based)

Main D4Science gateway: https://services.d4science.org



Use case: Protected Area Impacts Maps https://i-marine.d4science.org/web/protectedareaimpactmaps

Involved services and resources:

- (Authentication)
- (Authorization)
- Static web application
- Dataminer (Analytics engine)
- Geoserver
- Workspace
- FAIR



Terms of Use | Cookies Policy | Privacy Policy | Report an issue

BlueBRIDGE receives funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 67564

D4Science authentication and authorization flow (Keycloak, OIDC, federation)

Log		English v						
Loş		ci gibit -						
	g In							
rname or email		Academic / other						
sword	in	LinkedIn						
	G	Google						
Remember me Forgot Password?	У	Twitter						
Log In	۲	GitHub						
New user? Register Terms of Use Cookies Policy Privacy Policy Project Home D4Science is supporting the operation of a large set of diverse Initiatives, Communities of Practice, and Projects by offering VREs and Services.								
		— or —						
Q national research coun								
National Research Council (CNR)								





Copyright 2018-2021 - A

Support | Privacy Policy

5C portal is been jointly developed and maintained by the eInfraCentral, EOSC-hub and OpenAIRE-Advance projects funded by the European Horizon 2020 research and innovation programme with contribution of the European Commission.

D4Science authentication and authorization flow (Keycloak, orchestrator, VRE and users setup)

Conductor	start				Clients
Marco Lettere (out)	LAMBDA_TASK	Name * 🛛	Default Permission		
recutions	(init)				Lookup
All		Description 🚱			
Running	pyrest (authorize)	source Type 🕖	OFF		Search Q
Failed		Resources * 🕢	Default Resource		Client ID
Timed Out	pyrest	Apply Policy 😡	Select existing policy		%2Fd4science.research-infrastructures.eu
Terminated	(lookup_user)		Name	Description	%2Fd4science.research-infrastructures.eu%2FD4OS
Completed			VO-Admin_policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_AggregationMgmt
etadata	(select_user)		VRE-Manager_policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Lab
Workflow Defs			Catalogue-Admin_policy Data-Manager_policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Mappings
Tasks	pyrest (lookup_client)		Infrastructure-Manager_policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FARIADNEplus_Project
orkflow Events			Accounting-Manager_policy		%2Ed4science research-infrastructures eu%2ED4OS%2EArcheomar
Event Handlers	nyret		DataMiner-Manager_policy		
ask Queues	(get_client_roles)		VPE Decigner policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FArianna
Poll Data			Catalogue-Editor policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FBlue-CloudLab
	check_role_existance		Member_policy		%2Fd4science.research-infrastructures.eu%2FD4OS%2FBlue-CloudProject
	200				%2Fd4science.research-infrastructures.eu%2FD4OS%2FDisseminationEventsCollaboratory
		sion Strategy 🚱	Affirmative 🗸		%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCCollaboratory
	LAMBDA_TASK (select_role)		Save Cancel		%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillar4AgriFood
					%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillar4EarthScience
	pyrest (look_up_groups)				%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarITServiceRegistry
					%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarOS4SSCH
	LAMBDA_TASK				%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarOSTA
	(extract_group)				%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarResDataCtlg
	pyrest				%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarServiceRegistry
	(assign_user_to_group)				%2Fd4science.research-infrastructures.eu%2FD4OS%2FEOSCPillarTrainingAndSupport
	(final)				First Page Previous Page Next Page

The end Grazie!

Any questions?