INFN Cloud: security e policies

Massimo Sgaravatto
INFN Padova

Sommario

- Chi può usare INFN Cloud e cosa può fare
- AuthN, AuthZ
- Security recommendations

Premessa

- INFN Cloud non è una entità a se stante: fa parte dell'INFN, e ne segue quindi le regole
- Ci sono però alcune peculiarità e alcuni use case che non sono sempre chiaramente contemplati nelle attuali regole
  - Necessarie diverse interazioni con CCR e Harmony
- Policies e procedure non sono immutabili

Servizi INFN Cloud

Si possono classificare in 2 categorie:

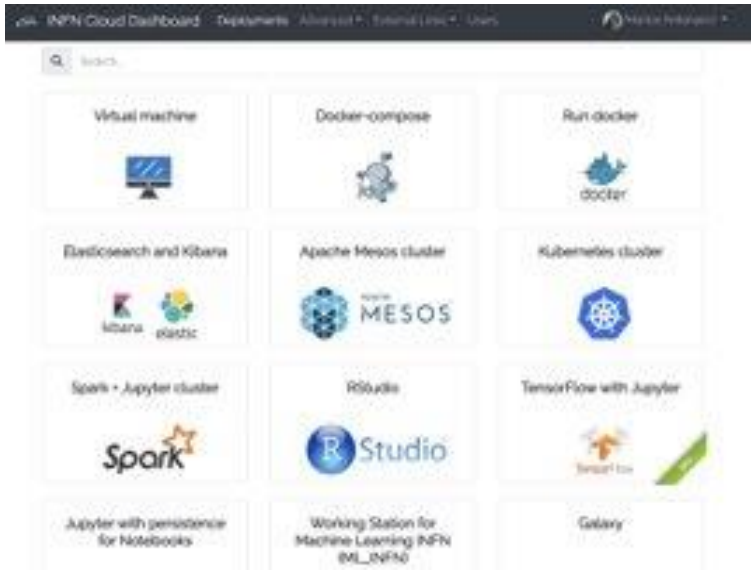
1. Servizi gestiti centralmente
   Es. Storage, Notebook as a Service

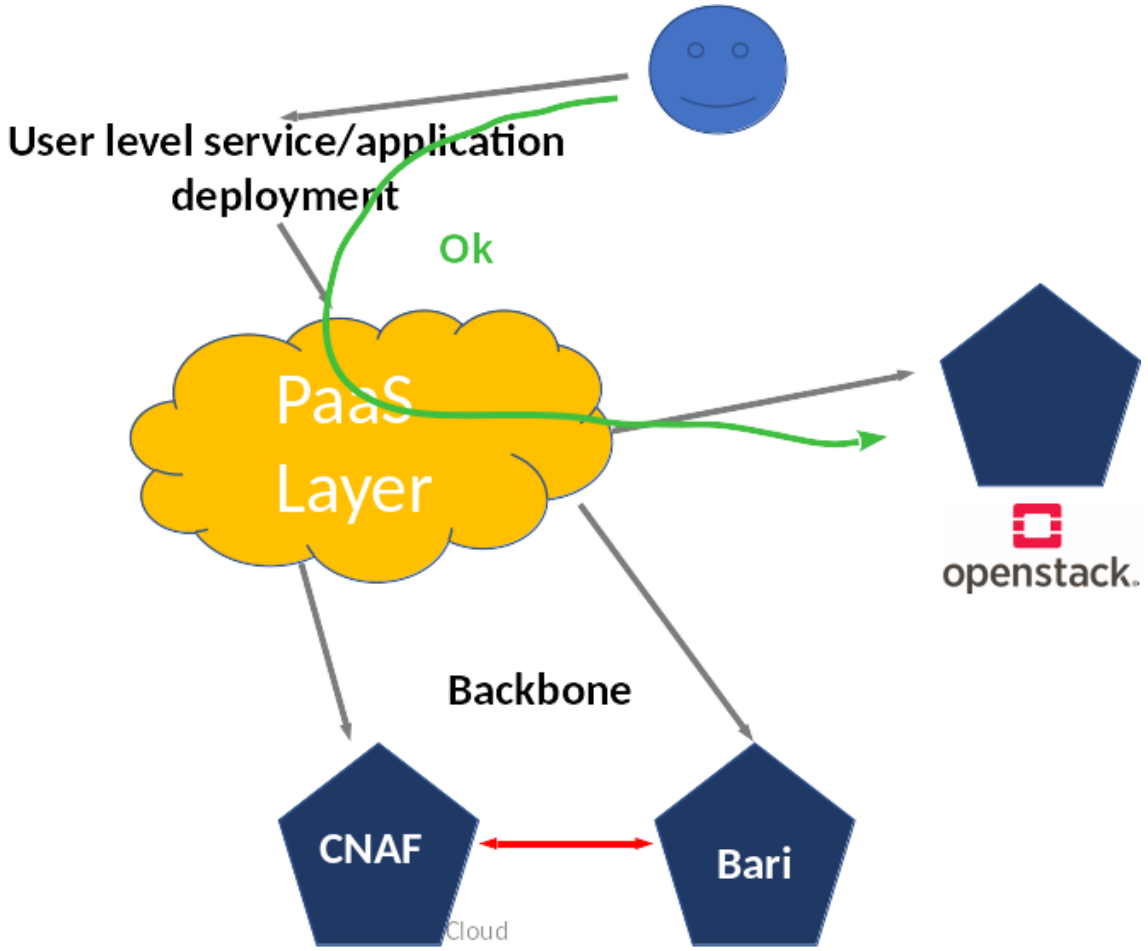
2. Servizi creati in modalità self service attraverso la dashboard di INFN Cloud

   a) Servizi su rete pubblica

   b) Servizi su rete privata
      - Solo outbound connectivity
      - Si accede al servizio attraverso una VPN

Accesso alle risorse di INFN Cloud

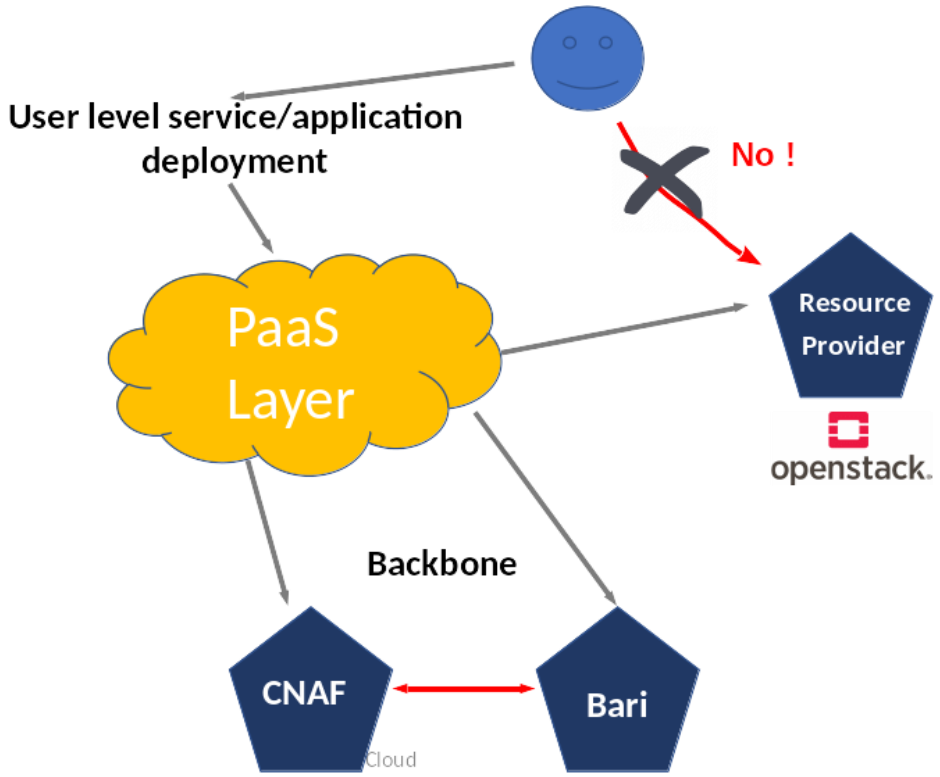




Si interagisce con il layer PaaS, che orchestra le risorse disponibili.

Sceglie un sito della federazione e li' istanzia il servizio

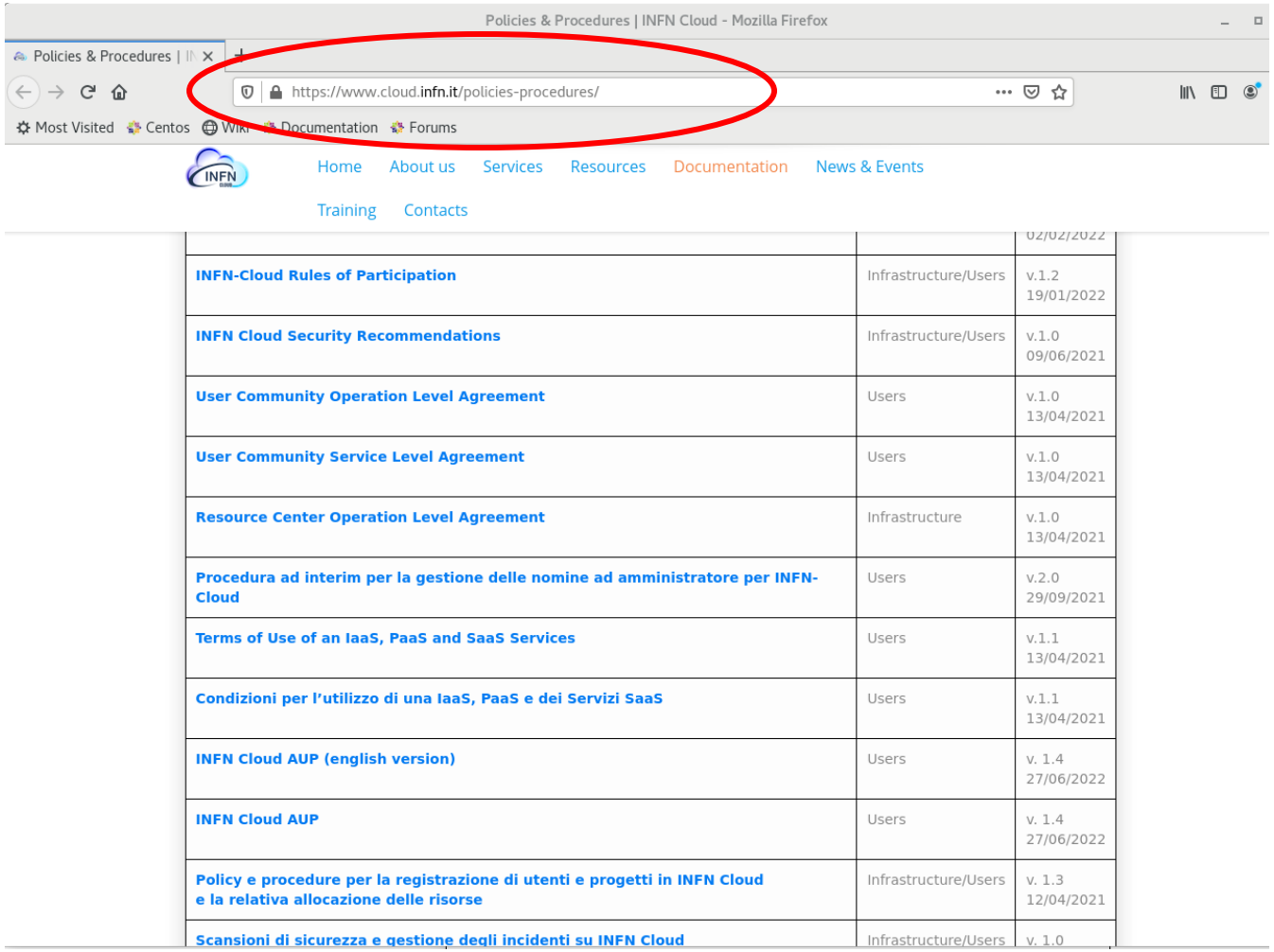
Accesso alle risorse di INFN Cloud (cont.ed)



Non si deve accedere direttamente alla IaaS (es. OpenStack) bypassando il layer PaaS

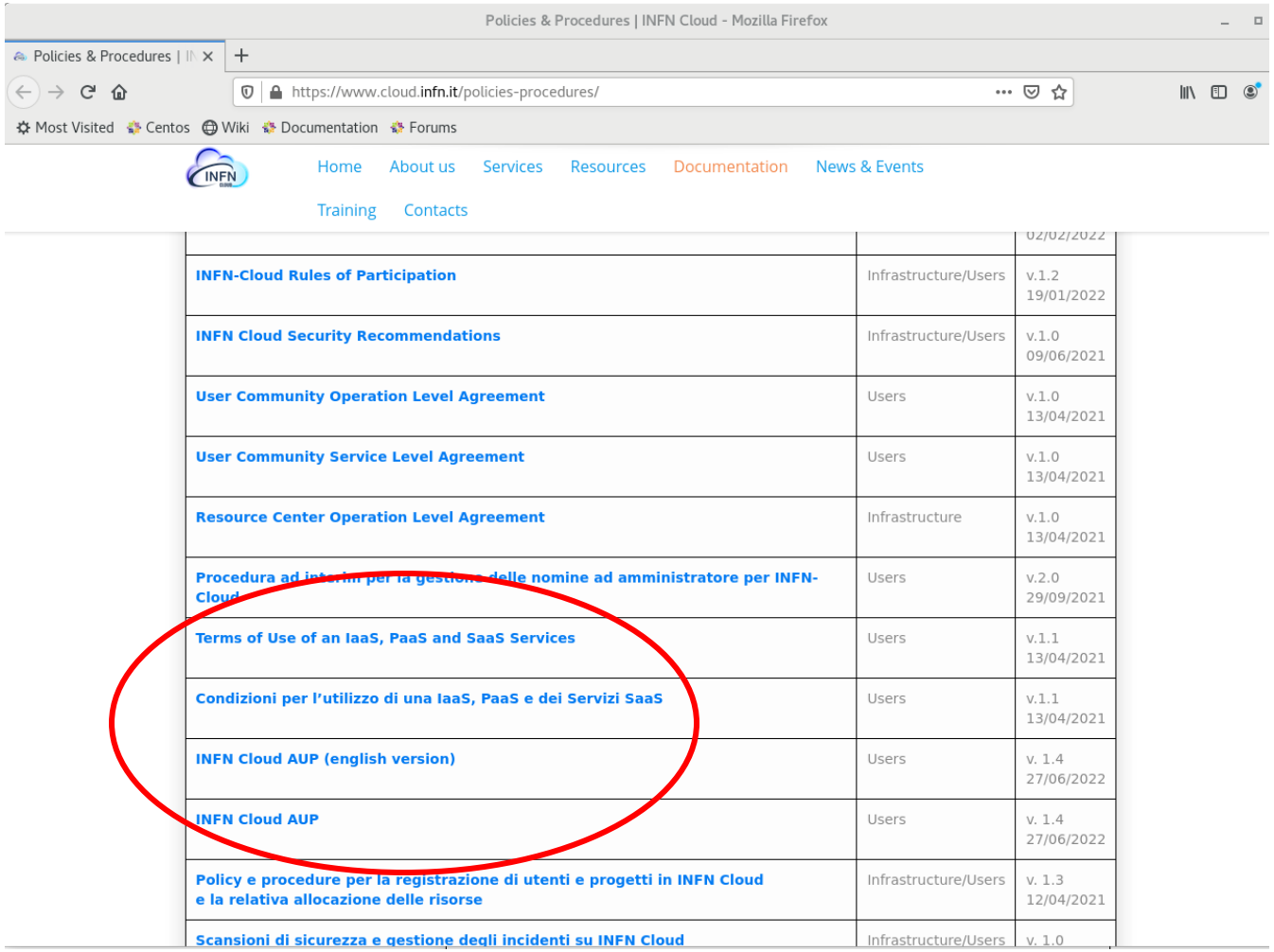
Eventuali eccezioni vanno discusse e concordate con il management di INFN Cloud

INFN Cloud: Policies e procedure



		02/02/2022
INFN-Cloud Rules of Participation	Infrastructure/Users	v.1.2 19/01/2022
INFN Cloud Security Recommendations	Infrastructure/Users	v.1.0 09/06/2021
User Community Operation Level Agreement	Users	v.1.0 13/04/2021
User Community Service Level Agreement	Users	v.1.0 13/04/2021
Resource Center Operation Level Agreement	Infrastructure	v.1.0 13/04/2021
Procedura ad interim per la gestione delle nomine ad amministratore per INFN-Cloud	Users	v.2.0 29/09/2021
Terms of Use of an IaaS, PaaS and SaaS Services	Users	v.1.1 13/04/2021
Condizioni per l'utilizzo di una IaaS, PaaS e dei Servizi SaaS	Users	v.1.1 13/04/2021
INFN Cloud AUP (english version)	Users	v. 1.4 27/06/2022
INFN Cloud AUP	Users	v. 1.4 27/06/2022
Policy e procedure per la registrazione di utenti e progetti in INFN Cloud e la relativa allocazione delle risorse	Infrastructure/Users	v. 1.3 12/04/2021
Scansioni di sicurezza e gestione degli incidenti su INFN Cloud	Infrastructure/Users	v. 1.0

INFN Cloud: AUP e Terms of Use



INFN-Cloud Rules of Participation	Infrastructure/Users	v.1.2 19/01/2022
INFN Cloud Security Recommendations	Infrastructure/Users	v.1.0 09/06/2021
User Community Operation Level Agreement	Users	v.1.0 13/04/2021
User Community Service Level Agreement	Users	v.1.0 13/04/2021
Resource Center Operation Level Agreement	Infrastructure	v.1.0 13/04/2021
Procedura ad interim per la gestione delle nomine ad amministratore per INFN-Cloud	Users	v.2.0 29/09/2021
Terms of Use of an IaaS, PaaS and SaaS Services	Users	v.1.1 13/04/2021
Condizioni per l'utilizzo di una IaaS, PaaS e dei Servizi SaaS	Users	v.1.1 13/04/2021
INFN Cloud AUP (english version)	Users	v. 1.4 27/06/2022
INFN Cloud AUP	Users	v. 1.4 27/06/2022
Policy e procedure per la registrazione di utenti e progetti in INFN Cloud e la relativa allocazione delle risorse	Infrastructure/Users	v. 1.3 12/04/2021
Scansioni di sicurezza e gestione degli incidenti su INFN Cloud	Infrastructure/Users	v. 1.0

AUP e Terms of Use

- Definiscono chi può usare INFN Cloud
- Definiscono cosa si può fare e cosa non si può fare (attività commerciali, spamming, mining, ecc.)
- Oggi ne vedremo un estratto
  - Con riferimento all'ultima versione delle AUP (v. 1.4)

Chi può usare INFN Cloud ?

- Dipendenti INFN
- Associati INFN
- Utenti "esterni" che ne hanno accesso in virtù di un progetto, contratto o convenzione con l'INFN

Utilizzatori di INFN Cloud

- Esistono 3 profili di utilizzatori di INFN Cloud:
  - Utente
    - Può usare servizi su INFN Cloud
  - Amministratore di servizio
    - Può creare e gestire servizi
  - Utente privilegiato
    - Può creare servizi ma solo su rete privata

Utente

- Può accedere e usare servizi su INFN Cloud (che qualcun altro ha creato e gestisce)
- Non può amministrare tali servizi
- Non può istanziare nuovi servizi
- Deve essere identificato tramite INFN-AAI o tramite un Identity Provider con un riconoscimento almeno di livello LoA2

Utente (cont.ed)

- Deve avere accettato:
  - AUP e Terms of Use di INFN Cloud
  - Disciplinare sull'uso delle risorse informatiche INFN

- Deve avere superato un corso di sicurezza informatica base almeno equivalente a quello INFN
  - Lista/criteri: saranno definiti da INFN CCR
  - Per il momento: l'unico corso "approvato" oltre a quello INFN è quello del CERN

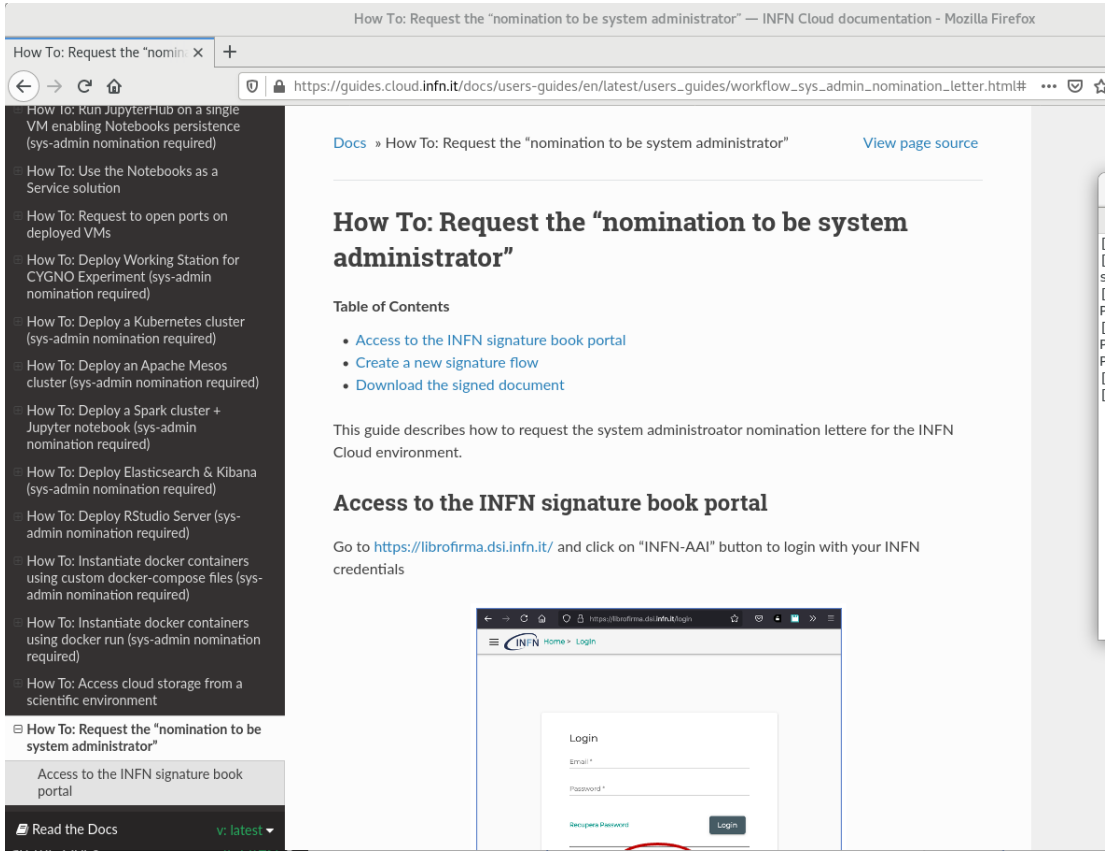
Amministratore di Servizio

- Può creare in modalità self service (attraverso la dashboard di INFN Cloud) nuovi servizi su INFN Cloud
- Diventa automaticamente amministratore dei servizi che ha istanziato
- Può dare accesso ai servizi che gestisce ad altri utenti
  - Deve però accertarsi che questi siano compliant con i vari requirement (accettazione AUP e disciplinare, corso base sicurezza informatica, ecc.)
  - Deve bloccare utenti che non sono più compliant
  - Deve conservare l'associazione tra account e identità degli utenti

Amministratore di Servizio (cont.ed)

- Oltre ai requisiti elencati per l'utente, deve avere ricevuto la nomina di amministratore di sistema (con scope "INFN Cloud quale utente amministratore") dal proprio Direttore
- Presuppone il possesso di tutte le conoscenze necessarie per amministrare una macchina
- Tale nomina è indipendente
  - dal sito dove i servizi saranno istanziati
  - dalla virtual organization (esperimento, gruppo, ecc.) di afferenza
- Almeno per il momento, la nomina ad amministratore di sistema la possono richiedere solo dipendenti e associati INFN

Nomina ad amministratore



La nomina ad amministratore si richiede attraverso un'applicazione basata sul libro firma INFN

Procedura documentata nella user guide di INFN Cloud

Utente privilegiato

- Può creare in modalità self service (attraverso la dashboard di INFN Cloud) nuovi servizi su INFN Cloud, ma solo su rete privata [*]

- Non serve la nomina ad amministratore di sistema ma:
  - NON è possibile dare accesso al servizio ad altri utenti
  - Il servizio deve trattare solo dati di tipo tecnico scientifico (il trattamento di dati personali NON deve essere significativo)

- Oltre ai requisiti elencati per l'utente, deve avere superato un corso intermedio di sicurezza informatica
  - In attesa che sia disponibile, per il momento va bene quello "base" INFN

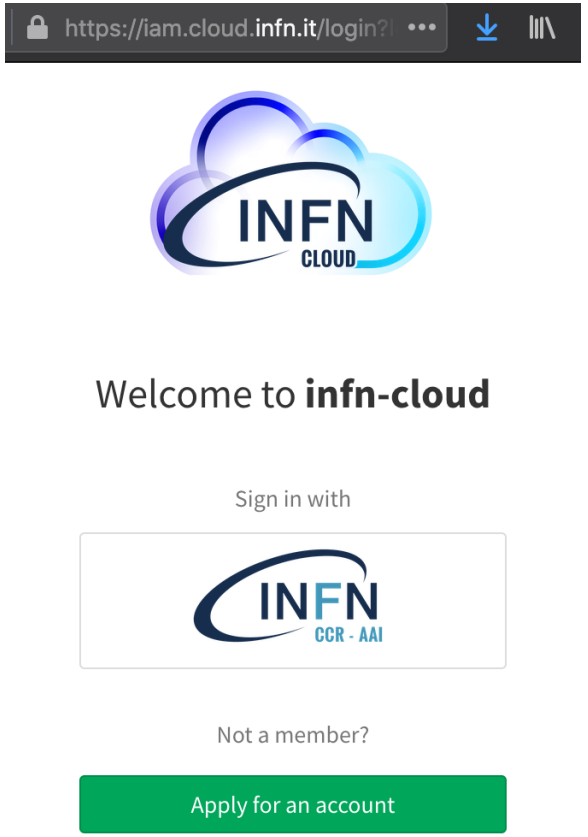
[*] no inbound connectivity
  - L'accesso al servizio avviene attraverso una VPN

Accesso alla rete

- Servizi su rete pubblica
  - Per default sono aperte inbound solo le porte strettamente necessarie all'uso del servizio istanziato
    - La porta 22 (SSH) è sempre aperta
  - Si può chiedere l'apertura di ulteriori porte all'atto della creazione del servizio
  - Eventualmente esiste una procedura per richiedere l'apertura di altre porte per servizi running
- Servizi creati su rete privata
  - Hanno solo outbound connectivity
  - Vi si accede attraverso una VPN (non controllata dall'utente)

AuthN / AuthZ

- L'autenticazione e autorizzazione ai core services di INFN Cloud viene gestita attraverso INDIGO IAM
- La richiesta di registrazione a INFN Cloud è una richiesta di registrazione all'istanza IAM di INFN Cloud (https://iam.cloud.infn.it)
- IAM può essere usato anche per gestire l'accesso ai servizi (almeno alcuni) istanziati dagli utenti amministratori



INDIGO IAM

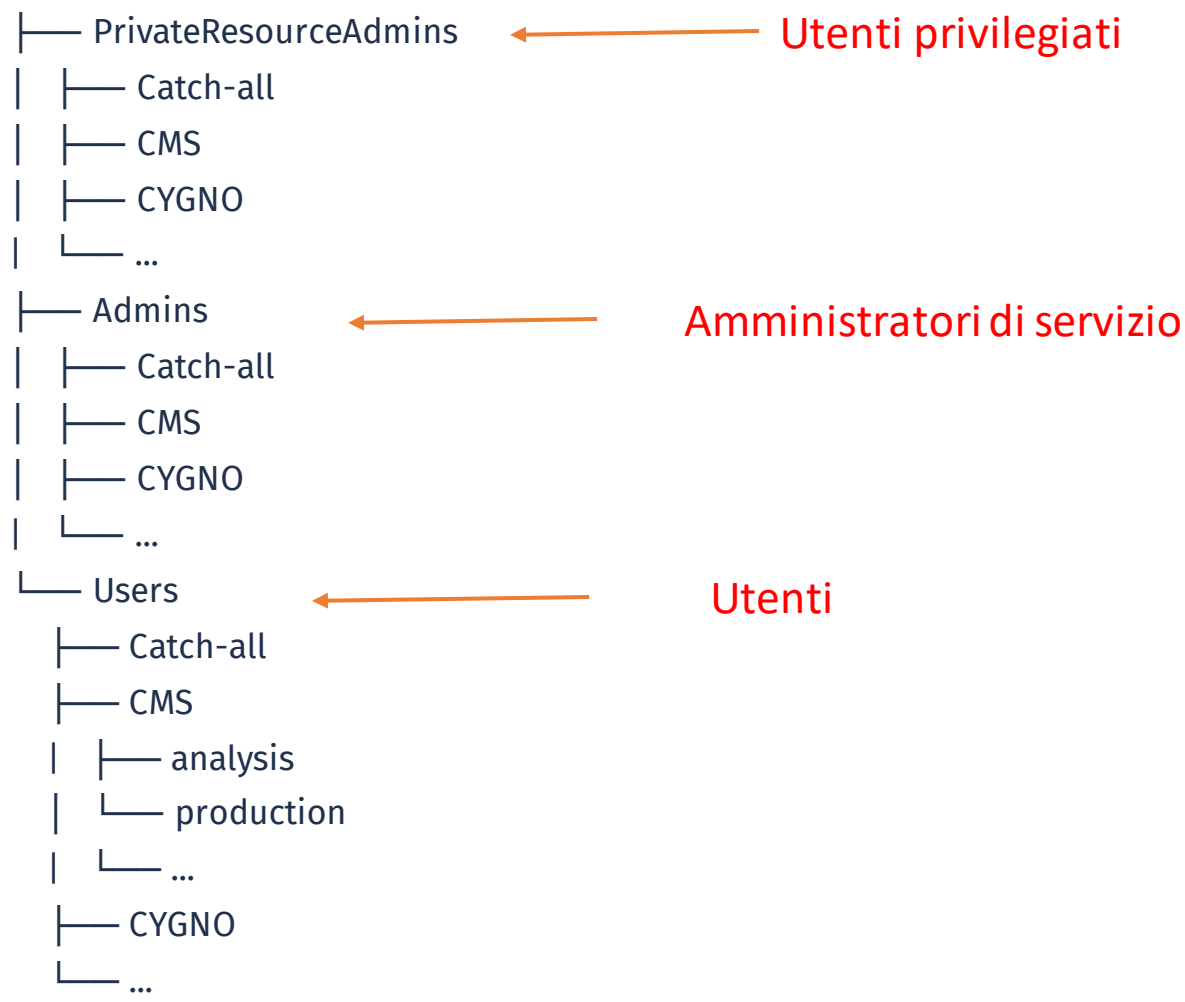
- Permette di gestire identità, group membership, policy di autorizzazione
- Compliant con OAuth e OpenID-Connect
- Supporta per l'autenticazione SAML IdPs, OpenID Connect, certificati X.509
- Soluzione scelta da WLCG come framework di Autenticazione e Autorizzazione

INFN Cloud IAM


```
├── PrivateResourceAdmins
│   ├── Catch-all
│   ├── CMS
│   ├── CYGNO
│   └── ...
├── Admins
│   ├── Catch-all
│   ├── CMS
│   ├── CYGNO
│   └── ...
└── Users
    ├── Catch-all
    ├── CMS
    │   ├── analysis
    │   └── production
    │   └── ...
    ├── CYGNO
    └── ...
```

Gli utilizzatori di INFN Cloud sono registrati secondo una gerarchia nello IAM di INFN Cloud (riorganizzazione in corso)

INFN Cloud IAM



Gli utilizzatori di INFN Cloud sono registrati secondo una gerarchia nello IAM di INFN CLoud (riorganizzazione in corso)

Amministrazione delle istanze

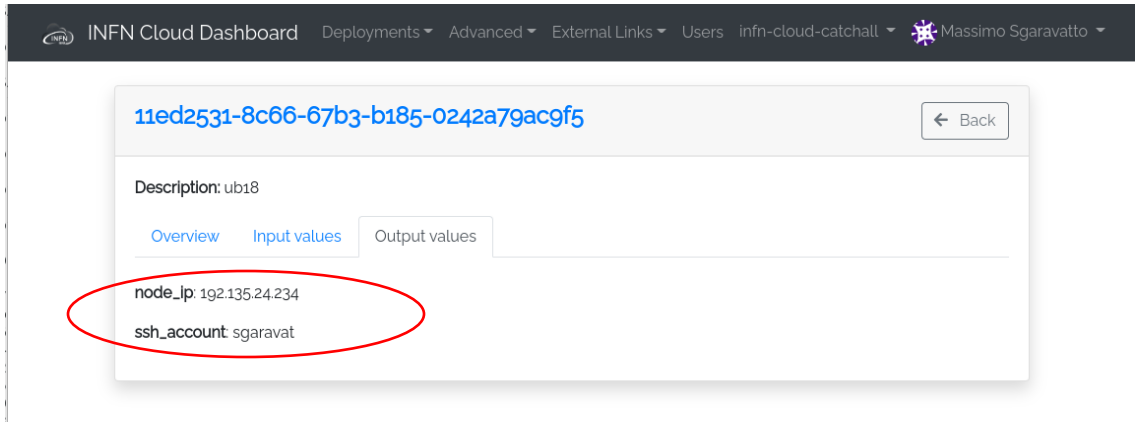
- Quando si crea un servizio in modalità self service attraverso la dashboard di INFN Cloud, è sempre possibile accedere alla VM (o alle VM) che ospita il servizio

- Accesso via SSH, attraverso chiave, che deve essere stata precedentemente creata/aggiunta [*]
  - Se il servizio è su rete privata serve prima attivare la VPN

- Una volta che si è acceduto alla VM, è possibile eseguire operazioni di system administration via sudo

[*] https://guides.cloud.infn.it/docs/users-guides/en/latest/users_guides/getting_started.html#ssh-keys

Amministrazione di istanze (cont.ed)




```
[sgaravat@lxsgaravat ~]$ ssh -i infncloud.pem sgaravat@192.135.24.234
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-189-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Sep  7 07:35:02 UTC 2022

  System load:  0.0               Processes:           86
  Usage of /:   21.9% of 9.51GB   Users logged in:     0
  Memory usage: 19%               IP address for ens3: 192.168.101.159
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

2 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


*** System restart required ***
Last login: Wed Sep  7 07:29:34 2022 from 193.205.157.174
sgaravat@vnode-0:~$ sudo apt-get update && sudo apt-get install linux-generic
Hit:1 http://nova.clouds.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://nova.clouds.archive.ubuntu.com/ubuntu bionic-updates InRelease

Hit:3 http://nova.clouds.archive.ubuntu.com/ubuntu bionic-backports InRelease

Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease

Reading package lists... Done
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  amd64-microcode crda intel-microcode iucode-tool iw libdbus-glib-1-2 libnl-3-200 libnl-g
enl-3-200 linux-firmware linux-image-generic
  linux-modules-extra-4.15.0-192-generic thermald wireless-regdb
The following NEW packages will be installed:
  amd64-microcode crda intel-microcode iucode-tool iw libdbus-glib-1-2 libnl-3-200 libnl-g
enl-3-200 linux-firmware linux-generic linux-image-generic
  linux-modules-extra-4.15.0-192-generic thermald wireless-regdb
0 upgraded, 14 newly installed, 0 to remove and 2 not upgraded.
Need to get 113 MB of archives.
After this operation, 527 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

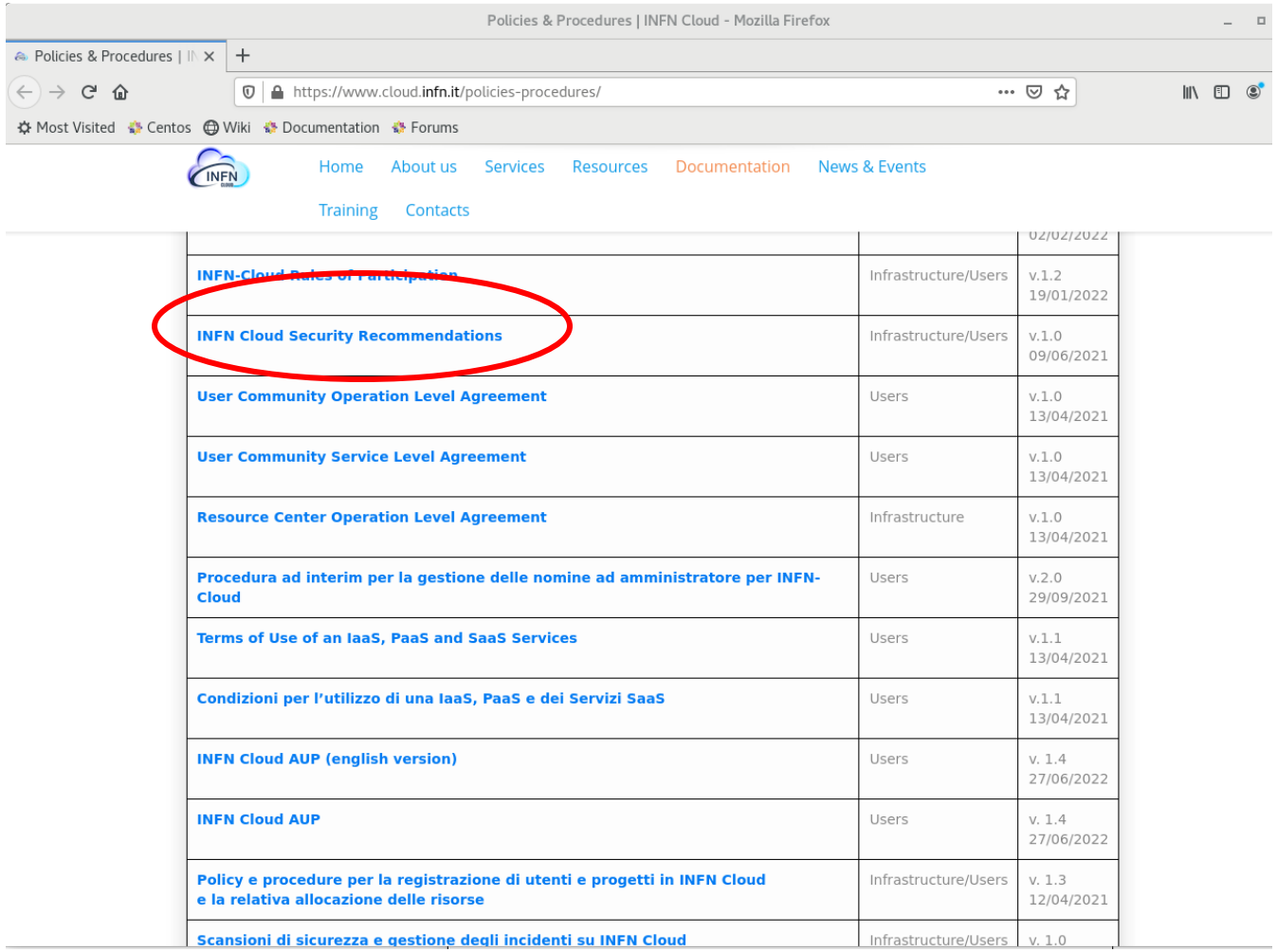
Amministrazione delle istanze (cont.ed)

- Ogni servizio istanziato su INFN Cloud deve sempre avere un amministratore che se ne fa carico
- Per default l'owner di un servizio (chi l'ha creato) ne è anche amministratore
- Un amministratore può aggiungere altri amministratori a un certo servizio
  - La definizione di un nuovo amministratore per un servizio deve essere notificata agli amministratori di INFN-Cloud aprendo un ticket sul service desk (https://servicedesk.cloud.infn.it)
  - Questo non vale per gli utenti privilegiati

Amministrazione delle istanze (cont.ed)

- I gestori dell'infrastruttura INFN Cloud gestiscono l'infrastruttura, ma non le VM e i servizi che gli utenti amministratori/utenti privilegiati istanziano su INFN Cloud
    - Non hanno nemmeno le credenziali per accedere a queste istanze

INFN Cloud: Security Recommendations



INFN-Cloud Rules of Participation	Infrastructure/Users	v.1.2 19/01/2022
INFN Cloud Security Recommendations	Infrastructure/Users	v.1.0 09/06/2021
User Community Operation Level Agreement	Users	v.1.0 13/04/2021
User Community Service Level Agreement	Users	v.1.0 13/04/2021
Resource Center Operation Level Agreement	Infrastructure	v.1.0 13/04/2021
Procedura ad interim per la gestione delle nomine ad amministratore per INFN-Cloud	Users	v.2.0 29/09/2021
Terms of Use of an IaaS, PaaS and SaaS Services	Users	v.1.1 13/04/2021
Condizioni per l'utilizzo di una IaaS, PaaS e dei Servizi SaaS	Users	v.1.1 13/04/2021
INFN Cloud AUP (english version)	Users	v. 1.4 27/06/2022
INFN Cloud AUP	Users	v. 1.4 27/06/2022
Policy e procedure per la registrazione di utenti e progetti in INFN Cloud e la relativa allocazione delle risorse	Infrastructure/Users	v. 1.3 12/04/2021
Scansioni di sicurezza e gestione degli incidenti su INFN Cloud	Infrastructure/Users	v. 1.0

Set di raccomandazioni che devono essere rispettate sui servizi istanziati su INFN Cloud

Se per qualche motivo non si riescono a implementare, la cosa va discussa con INFN Cloud WP4 per vedere come gestire il problema

Security Recommendations

Esempi:

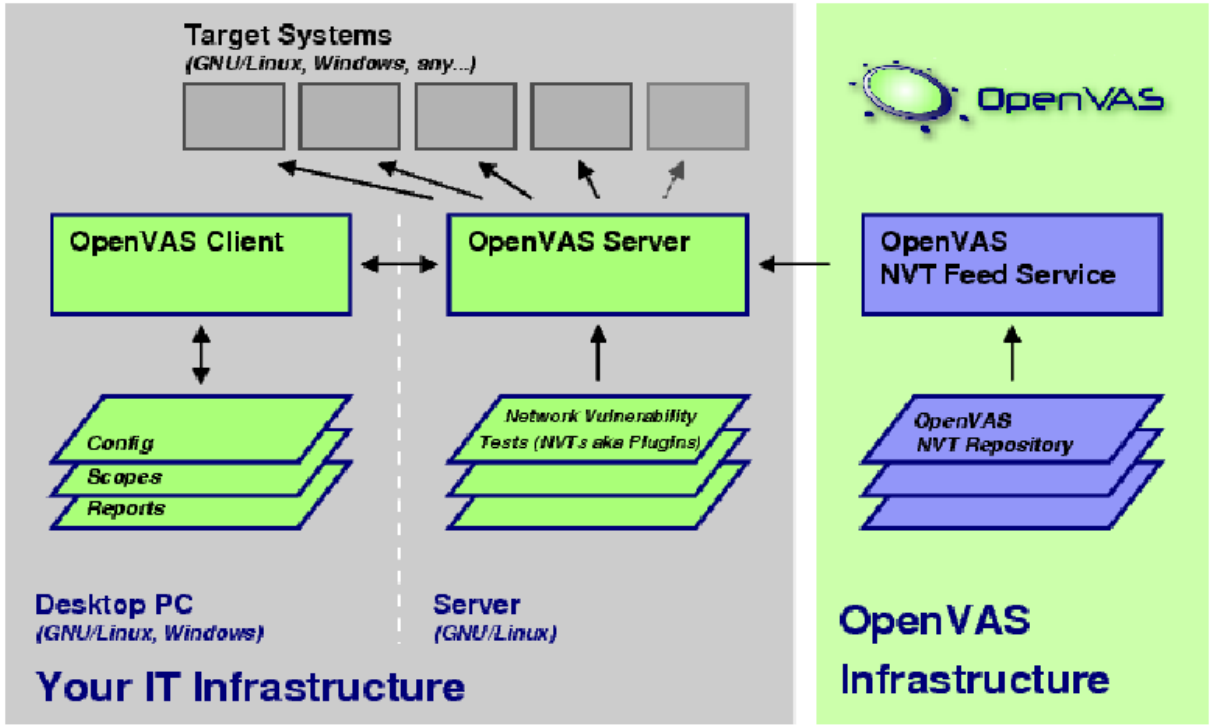
- Mantenere sempre aggiornato il Sistema Operativo
- Gestire sempre autenticazione ed autorizzazione degli utenti
- Non usare credenziali di default
- Criptare tutte le comunicazioni
- Esporre solo quello che è strettamente necessario
  - Chiudere le porte di rete che non servono
- Configurare SSH attraverso chiave (no password login)

Vulnerabilità e incidenti di sicurezza in INFN Cloud

- Vengono fatte periodicamente scansioni di sicurezza sulle istanze
- In INFN Cloud il coordinamento per la gestione delle vulnerabilità e incidenti di sicurezza (attacchi) è affidata al Security Incident Team (SIT)
- Implementando le procedure e direttive definite dal WP4 di INFN Cloud (Security, Policies & Procedures)
- In compliance con le procedure e direttive INFN sull'uso delle risorse informatiche

Vulnerability scan

- Effettuate attraverso OpenVAS (GreenBone)
- Rileva eventuali vulnerabilità sui servizi esposti dalle istanze



Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Jan 9 03:05:08 2020	Done	Immediate scan of IP 192.168.11.137	N/A	0	0	0	0	0	

Report: Results (312 of 734)

ID: 97cc63d0-65d7-45ee-8ca8-711df1baa7dd
Modified:
Created:
Owner: admin

1 - 100 of 312

Vulnerability	Severity	QoD	Host	Location	Actions
rexec Passwordless / Unencrypted Cleartext Login	10.0 (High)	75%	192.168.11.137	512/tcp	
Samba End Of Life Detection	10.0 (High)	75%	192.168.11.137	445/tcp	
Samba 'TALLOC_FREE()' Function Remote Code Execution Vulnerability	10.0 (High)	75%	192.168.11.137	445/tcp	
PHP Multiple Vulnerabilities - Aug08	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP Version < 5.2.7 Multiple Vulnerabilities	10.0 (High)	75%	192.168.11.137	80/tcp	
PHP End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	80/tcp	
MySQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	3306/tcp	
PostgreSQL End Of Life Detection (Linux)	10.0 (High)	75%	192.168.11.137	5432/tcp	

Se il vulnerability scanner trova un problema da curare in una istanza …

… Il SIT apre un ticket notificando il rispettivo utente-amministratore

---

Dear user,

You are the owner of a VM called server-aa0fb6da-101a-11ec-91f3-fa163e5257b7 (ip address: 192.135.24.144) which is deployed on the INFN Cloud infrastructure.
During the latest security scan, a vulnerability scored 5.0/10 has been found. Here the details:

'Vulnerable' cipher suites accepted by this service via the TLSv1.0 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.1 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

'Vulnerable' cipher suites accepted by this service via the TLSv1.2 protocol:

TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)
TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

Report prodotto da OpenVAS con i dettagli del problema e come risolverlo

---

The whole report for your VM is attached to this message as a pdf file.

You are expected to solve this issue before March 24, 2022. Feel free to send an e-mail to security@cloud.infn.it if you need help or advice on fixing this issue.

Thanks, the INFN Cloud Incident Team.

Risolvere la vulnerabilità nell'istanza

- E` responsabilità dell'utente-amministratore che gestisce quell'istanza

- E` l'unico che ha i privilegi amministrativi per farlo
  - Gli amministratori di INFN Cloud non hanno accesso alle vostre istanze

- Va fatto entro i tempi indicati nel mail mandato dal SIT

Risolvere la vulnerabilità nell'istanza

- Va sempre fatto, anche se l'istanza non è critica e non contiene dati "critici"
  - La vulnerabilità può avere impatto anche su altri sistemi di altri utenti
  - Un incidente di sicurezza può avere ripercussioni su INFN Cloud e sull'Ente (es. reti INFN potrebbero essere "bannate")

Tempi di risoluzione

Gravità	Vulnerabilità indicata dalla scansione	Tempo limite
Critica	9,10	<= 1 settimana
Alta	6,7,8	6 settimane
Media	4,5	6 mesi
Bassa	1,2,3	8 mesi

Il tempo limite è comunque specificato nel mail inviato dal SIT

La gravità (e relativo tempo limite) di una vulnerabilità può cambiare

Scansioni autenticate

- Per default viene fatta una scansione sui servizi esposti

- Esiste la possibilità di effettuare scansioni autenticate, che fanno anche un controllo dall'interno del sistema
  - Permettono un'analisi delle vulnerabilità molto più accurata

- Per il momento l'abilitazione delle scansioni autenticate è su base volontaria

Scansioni autenticate (cont.ed)

- Per abilitare le scansioni autenticate sull'istanza che si gestisce:

```
sudo su -
wget https://baltig.infn.it/infn-cloud/users_utils/-/raw/main/enable-authenticated-scans.sh
chmod +x enable-authenticated-scans.sh
./enable-authenticated-scans.sh
```

Lo script:

- Crea utente non privilegiato
- Abilita l'accesso a questo utente via chiave SSH ma solo dai server OpenVAS

Vulnerabilità non rilevate da OpenVAS

- Viene mandato un mail (in genere a tutti gli utenti) per segnalare il problema

- Nel mail è indicato
  - Il tipo di servizio coinvolto
  - Le action necessarie
  - Il tempo limite per applicarle

Esempio

```
--------------------------------------------------------------------------------

An English version of this message follows the Italian one

--------------------------------------------------------------------------------

Sono state annunciate due vulnerabilita` del kernel linux (CVE-2021-22555 e CVE-2021-3715) che possono permettere a un utente di ottenere accesso privilegiato.

Attenzione: si tratta di due vulnerabilita` diverse rispetto alla vulnerabilita` CVE-2021-33909 di cui vi avevamo riportato a Luglio.


Azioni richieste
================

Gli amministratori di servizio che hanno istanziato uno o piu' servizi "Virtual Machine" devono aggiornare il kernel di queste macchine virtuali facendo riferimento alle istruzioni riportate sot
Questo deve essere fatto entro 6 settimane


Istruzioni per virtual machine Centos7
--------------------------------------

Dare il comando:


uname -r


Se viene riportata una versione del kernel maggiore o uguale a 3.10.0-1160.42.2, la macchina virtuale non presenta queste vulnerabilita`.
In caso contrario, per aggiornare il kernel si puo` usare il seguente comando (il comando potrebbe non aggiornare nessun pacchetto se il nuovo kernel e` stato gia` installato dal sistema di aggi


sudo yum clean all && yum -y update kernel*


Per abilitare l'uso del nuovo kernel, e` necessario un reboot:
```

Vulnerabilità non risolta

- Se la vulnerabilità in una istanza non viene curata nei tempi prestabiliti, viene isolata
- Viene rimessa in rete solo quando la vulnerabilità viene risolta
- Viene anche sospeso l'account del relativo utente-amministratore (per evitare che possa riaccendere l'istanza)

Grazie per l'attenzione !

Backup slides

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT)
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

INFN Cloud WP1 e site admin

Responsabili di gestire in maniera sicura e tenere aggiornati i vari servizi dell'infrastruttura

Responsabili di fornire e tenere aggiornate le immagini che vengono usate per le istanze degli utenti

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

INFN Cloud WP5

Responsabili di fornire e tenere aggiornati i vari servizi, configurandoli nella maniera più sicura possibile

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Team (SIT) e WP4 di INFN Cloud
- INFN CSIRT
- I gestori dell'infrastruttura
- Gli sviluppatori dei servizi
- L'utente amministratore

Responsabile di gestire in maniera sicura le istanze amministrate

Responsabile di applicare le istruzioni comunicate dal SIT/CSIRT

INFN Cloud Security Incident Team (SIT)

- Composizione attuale
  - Marica Antonacci (BA)
  - Vincenzo Ciaschini (CNAF)
  - Alessandro Italiano (BA)
  - Gianluca Peco (BO)
  - Massimo Sgaravatto (PD)
  - Stefano Stalio (LNGS)

security@cloud.infn.it

Un mail inviato a questo indirizzo crea un ticket

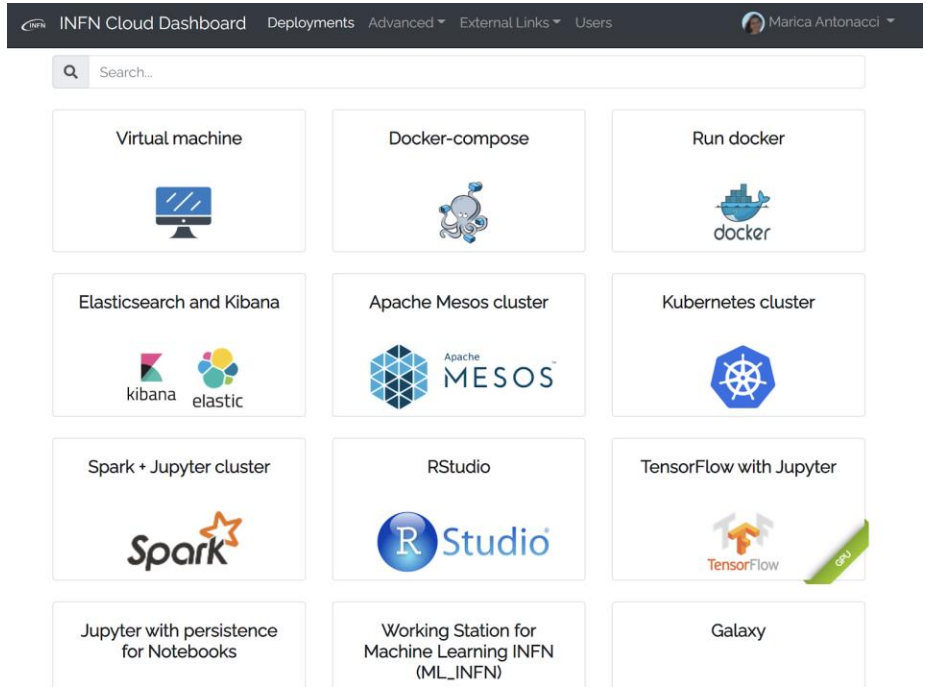
Per favore non cambiate subject rispondendo a un mail

Rilevazione delle vulnerabilità

- Il SIT viene a conoscenza di vulnerabilità (vere o presunte) in diversi modi:
  - Vulnerability scan
  - Notifiche da GARR-CERT (via APM), INFN-CSIRT, ecc.. su vulnerabilità in specifiche istanze
  - Annunci di vulnerabilità in specifici software

Vulnerability scan

- Ogni servizio del catalogo di INFN Cloud viene controllato wrt la presenza di vulnerabilità prima di essere messo in produzione
- Questo però non è chiaramente sufficiente
  - Una vulnerabilità può essere scoperta dopo
  - Una vulnerabilità può essere stata introdotta da una configurazione/installazione fatta successivamente alla creazione del servizio



Vulnerability scan

-  Il vulnerability scanner controlla periodicamente tutte le istanze su INFN Cloud

- Scansione fatta almeno 1 volta a settimana, di notte

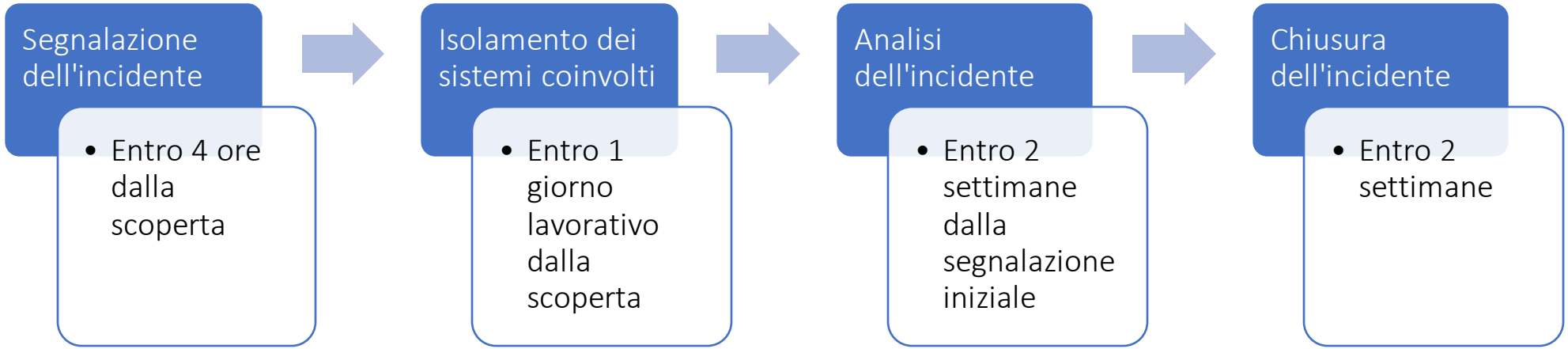
- Scansione configurata in modo da minimizzare l'impatto

Conferma esplicita

- Nel caso di vulnerabilità critiche o che abbiano impatto rilevante, il SIT può chiedere esplicita conferma che siano state applicate le indicazioni date

- La non risposta è interpretata come il non avere risolto la vulnerabilità nei tempi stabiliti

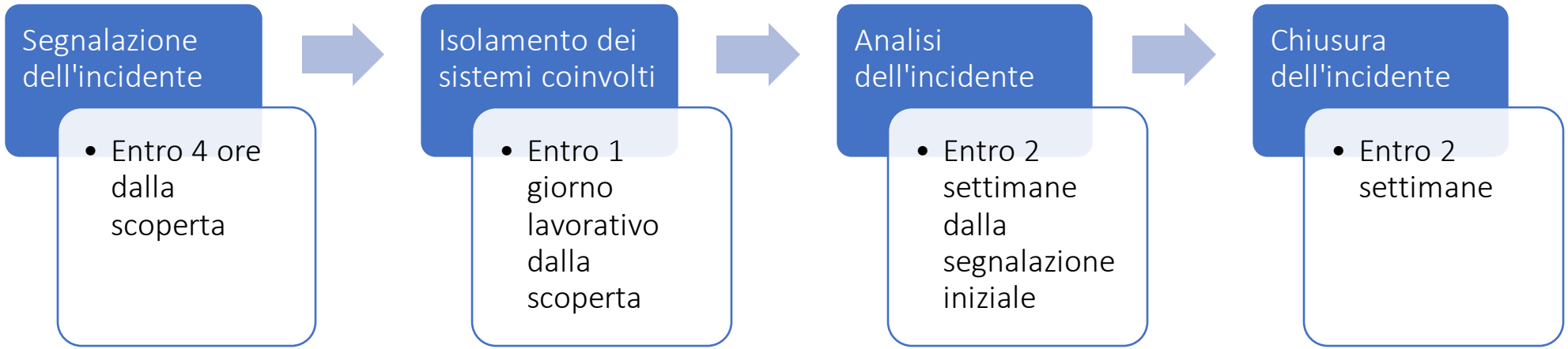
Gestione di un incidente (attacco)



Gestione di un incidente (attacco)

Chi scopre un incidente (vero o sospetto) deve comunicarlo subito al SIT

Il SIT informa l'INFN CSIRT

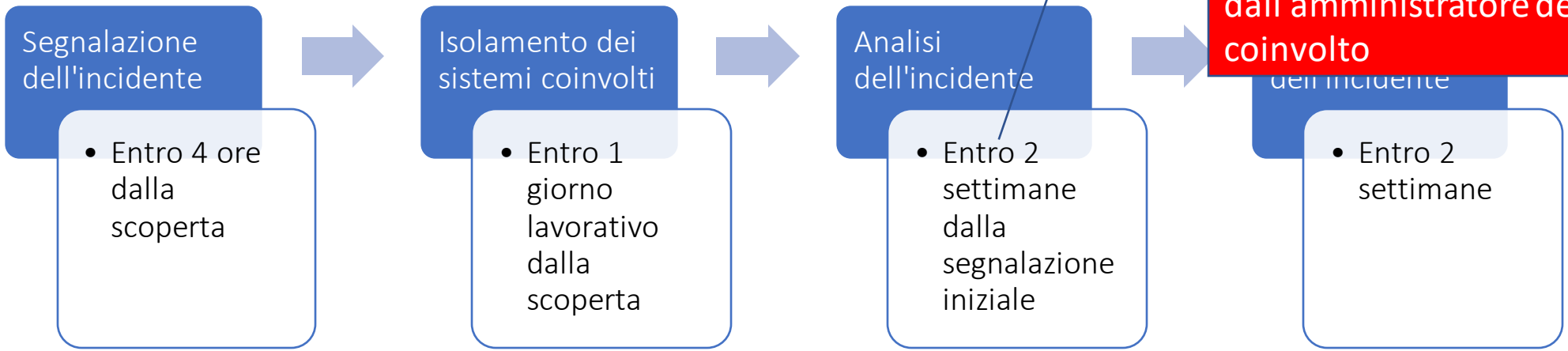


Gestione di un incidente (attacco)

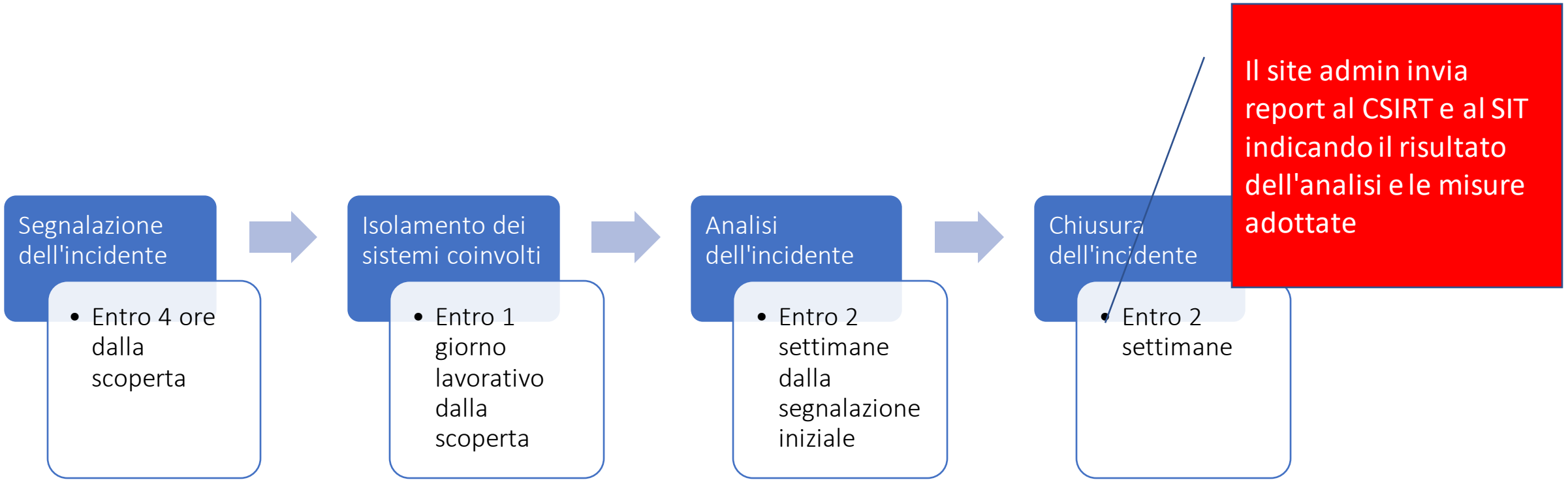
Gestione di un incidente (attacc

- Da dove è partito l'attacco ?
- Evidenze di compromissione ?
- Vulnerabilità sfruttate ?
- Tipo di attacco ?
- Cosa ha fatto l'attaccante ?
- Dati compromessi ?
- Account compromessi ?

Da parte del site admin e dall'amministratore del sistema coinvolto



Gestione di un incidente (attacco)



Riferimenti

- INFN Cloud Policies & Procedures

  https://www.cloud.infn.it/policies-procedures/

  - Scansioni di sicurezza e gestione degli incidenti su INFN CLOUD

- INFN CSIRT web site

  https://www.csirt.infn.it

- INFN DPO (Data Protection Officer) web site

  https://dpo.infn.it/

Logging

Le istanze sono preconfigurate per mandare i log verso server centrali

Non modificare questa configurazione !

"Riabilitazione" di una istanza isolata

1. L'utente amministratore comunica l'indirizzo IP da cui si collegherà
2. Il site admin riaccende l'istanza abilitandone l'accesso solo dall'IP indicato dall'utente amministratore
3. L'utente amministratore si collega alla istanza e risolve la vulnerabilità
4. Il site admin ripristina il setting di rete originario dell'istanza
5. L'utente amministratore viene riabilitato nel gruppo IAM dove era stato prima rimosso

Data Breach

- Violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati

- Può avvenire a seguito di un attacco informatico ma può avere altre cause (es. furto o smarrimento di un dispositivo informatico)

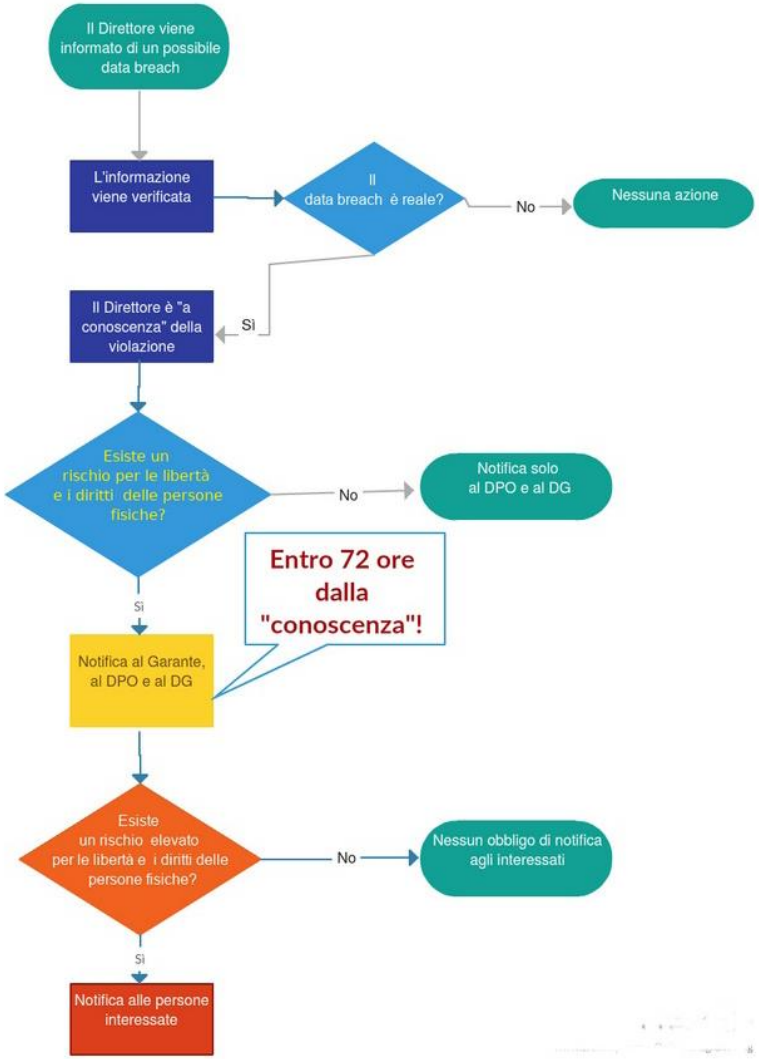
Dati personali

Qualsiasi informazione riguardante una persona fisica («interessato») identificata o identificabile

V. "Norme per il trattamento di dati personali nell'INFN" *

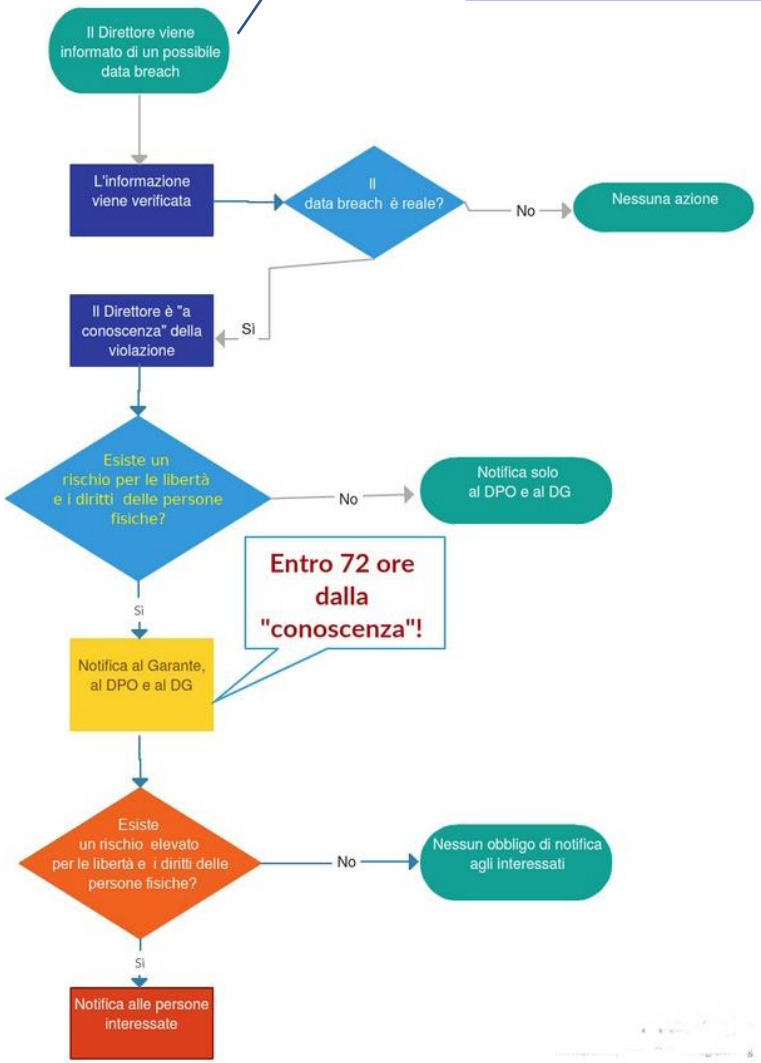
* https://dpo.infn.it/wp-content/uploads/2018/12/Norme_Trattamento_Dati_Personali_INFN.pdf

INFN Data Breach procedure



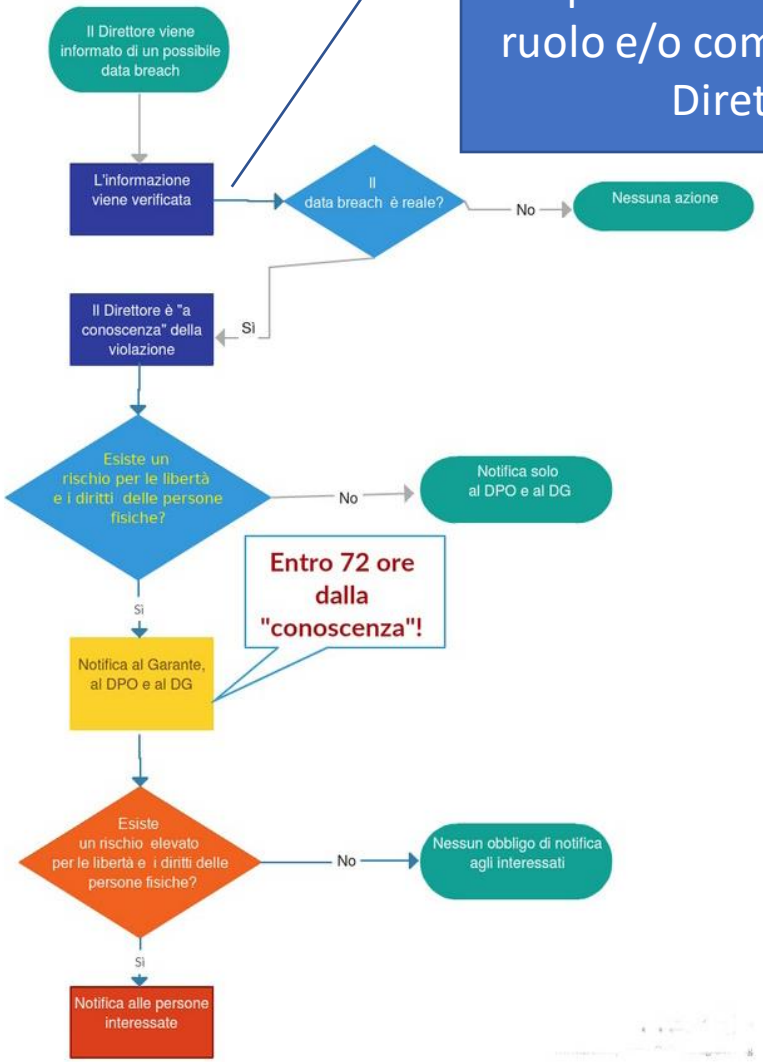
INFN Data Breach proc

Chi e` a conoscenza di un data breach (reale o sospetto) deve avvertire Direttore e referente locale del DPO

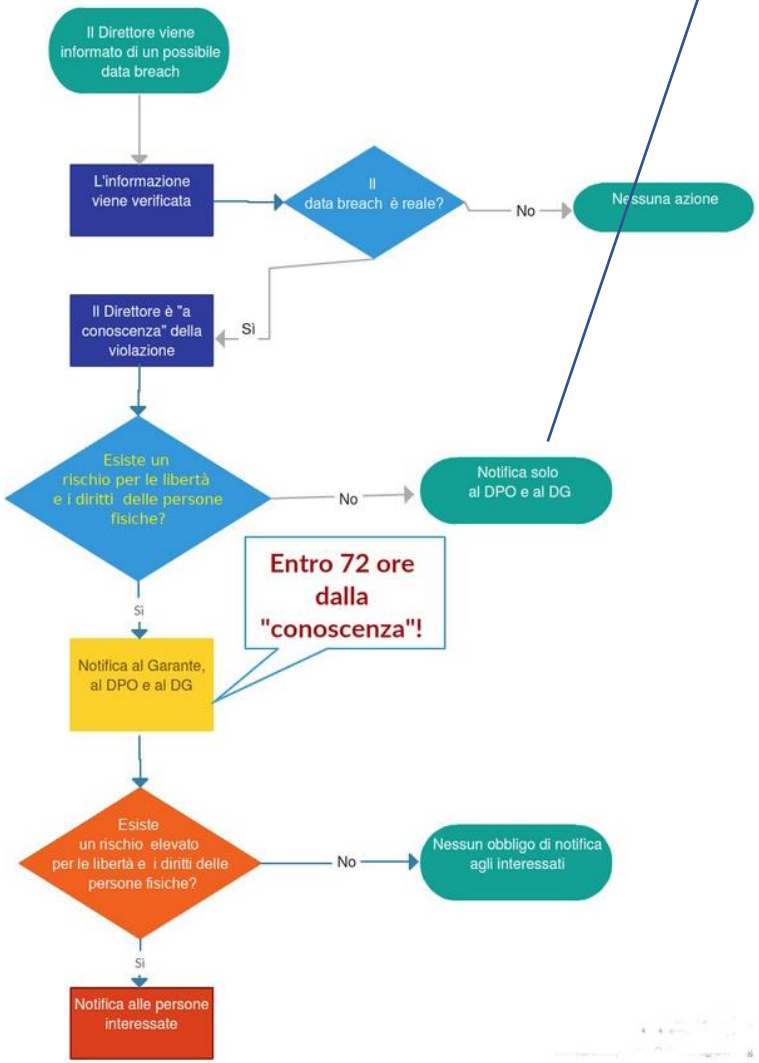


INFN Data Breach procedure

Data breach viene verificato da persone incaricate (per ruolo e/o competenza) dal Direttore

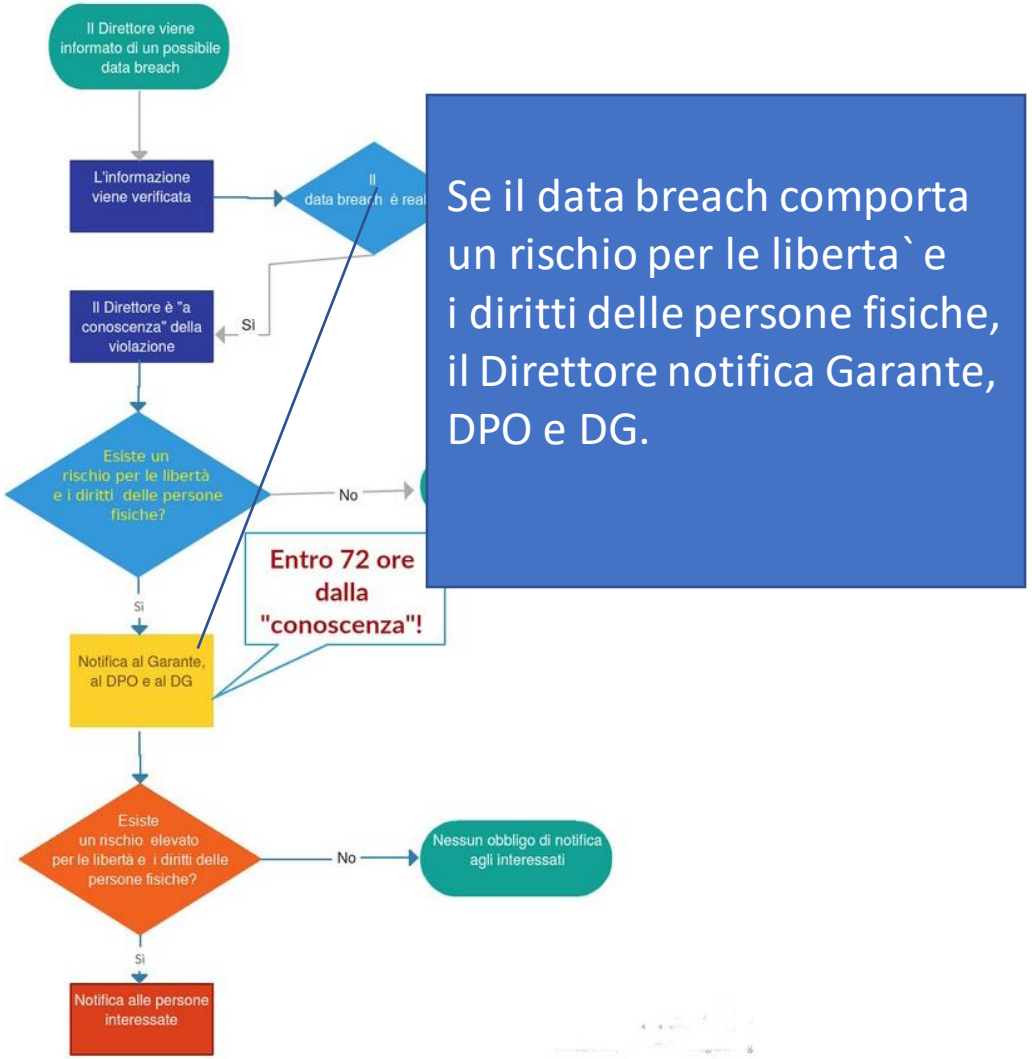


INFN Data Breach procedure



Se il data breach non comporta un rischio per le liberta` e i diritti delle persone fisiche, il Direttore notifica DPO e DG. Viene indicato il risultato dell'analisi e le azioni da intraprendere

INFN Data Breach procedure

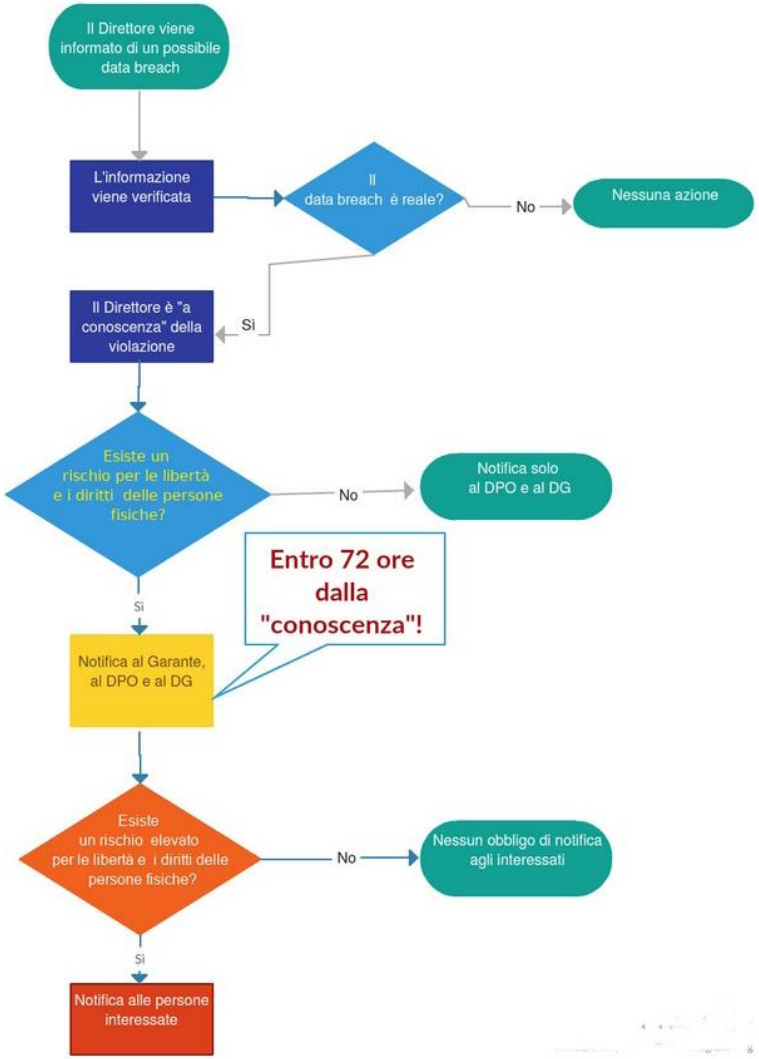


Se il data breach comporta un rischio per le liberta` e i diritti delle persone fisiche, il Direttore notifica Garante, DPO e DG.

INFN Data Breach procedure

Se c'e` un rischio elevato per le liberta` e i diritti delle persone fisiche, il Direttore informa gli interessati sulle conseguenze della violazione e sulle azioni che verranno intraprese

INFN Data Breach procedure



Il Direttore notifica il CSIRT

Il Direttore eventualmente provvede alla denuncia all'autorita` giudiziaria

Vulnerabilità e incidenti: attori coinvolti

- Security Incident Te…oud
- INFN CSIRT
- I gestori dell'infrastruttura INFN Cloud
- Gli sviluppatori dei servizi INFN Cloud
- L'utente amministratore

Offre sostegno nella prevenzione e gestione degli incidenti di sicurezza

Stretto coordinamento tra SIT e CSIRT