Sicurezza e rischio informatico su INFN Cloud

Lavorare sul proprio laptop/desktop vs (INFN-)CLOUD

Gianluca Peco, Stefano Stalio, Paolo Veronesi

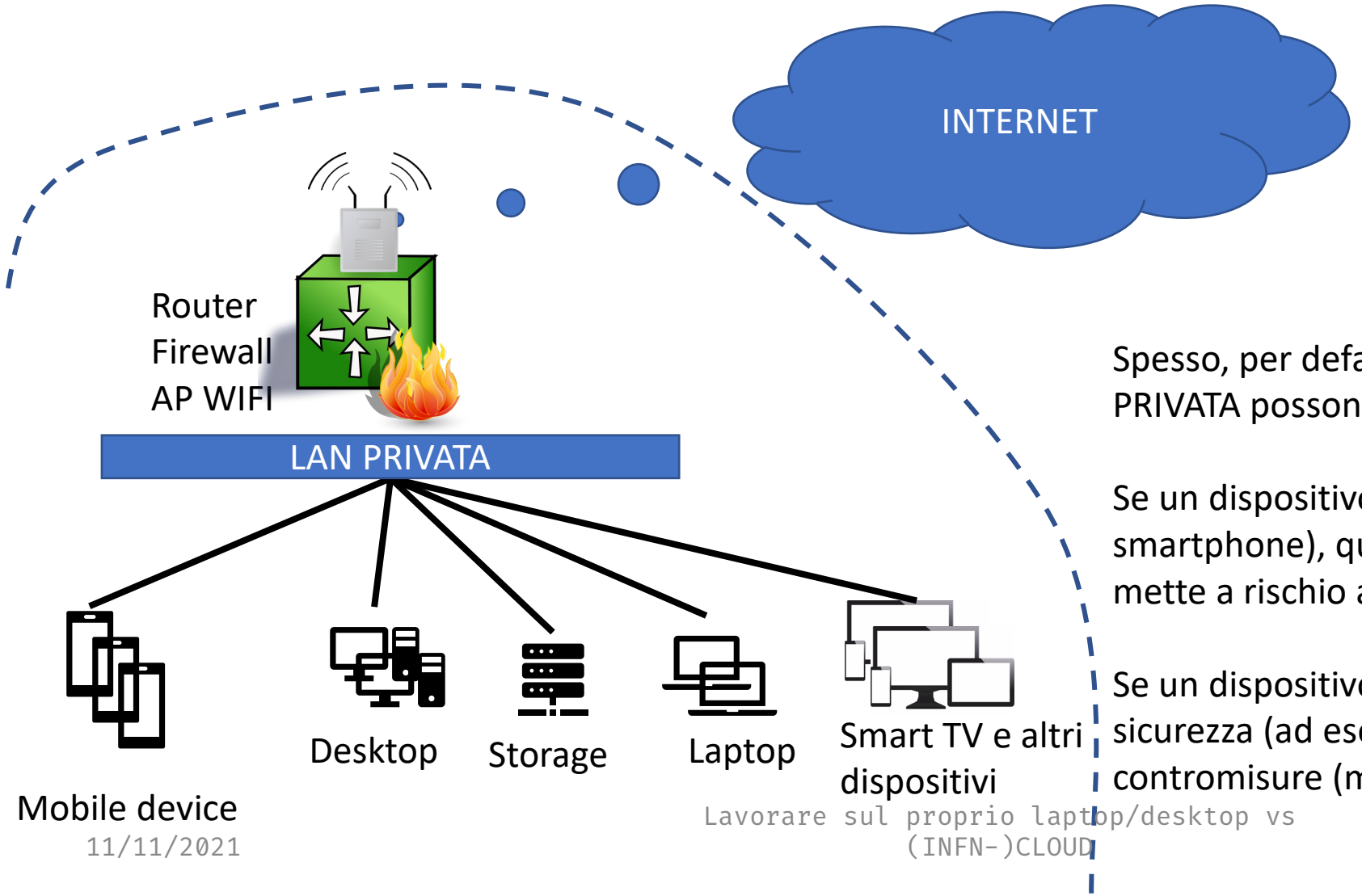
Obiettivo consapevolezza

- In qualità di **utenti**, abbiamo una serie di regole e policy a cui dobbiamo attenerci
  - le abbiamo ripassate dettagliatamente nella prima giornata
- Quando si è **amministratori di sistema** le regole e le responsabilità aumentano e occorre tenere presente l'ambiente nel quale i sistemi sono inseriti
  - Ma alcune regole valgono ovunque:
    - Tenere S.O. e Applicativi aggiornati
    - Esporre solo quanto deve essere esposto pubblicamente
    - Misure Minime
  - Esistono delle best practice
    - Per ogni S.O.
    - Per ogni Applicativo
    - Per ogni oggetto su cui si lavora (vm, docker container, k8s, etc)

Sommario

- Descrizione ambienti di lavoro
  - Casa
  - Ufficio
  - Cluster di calcolo
- Use case in vari ambienti di lavoro
  - Aggiornamento S.O.
  - Installazione/Aggiornamento di un servizio
  - Esposizione del servizio

pc/laptop @ home



Spesso, per default, tutti i dispositivi connessi alla LAN PRIVATA possono «vedersi» tra di loro e comunicare

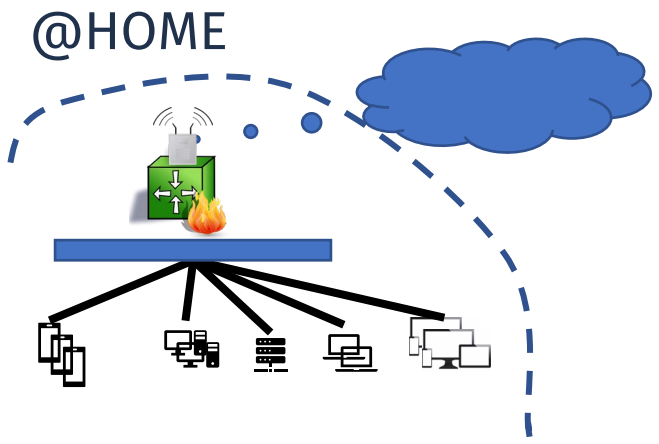
Se un dispositivo viene compromesso (ad esempio lo smartphone), quando questo si trova nella LAN PRIVATA mette a rischio anche tutti gli altri

Se un dispositivo non riceve più aggiornamenti di sicurezza (ad esempio una smart TV), vanno prese delle contromisure (mitigazione del rischio)

@HOME: Policy del provider e vostre

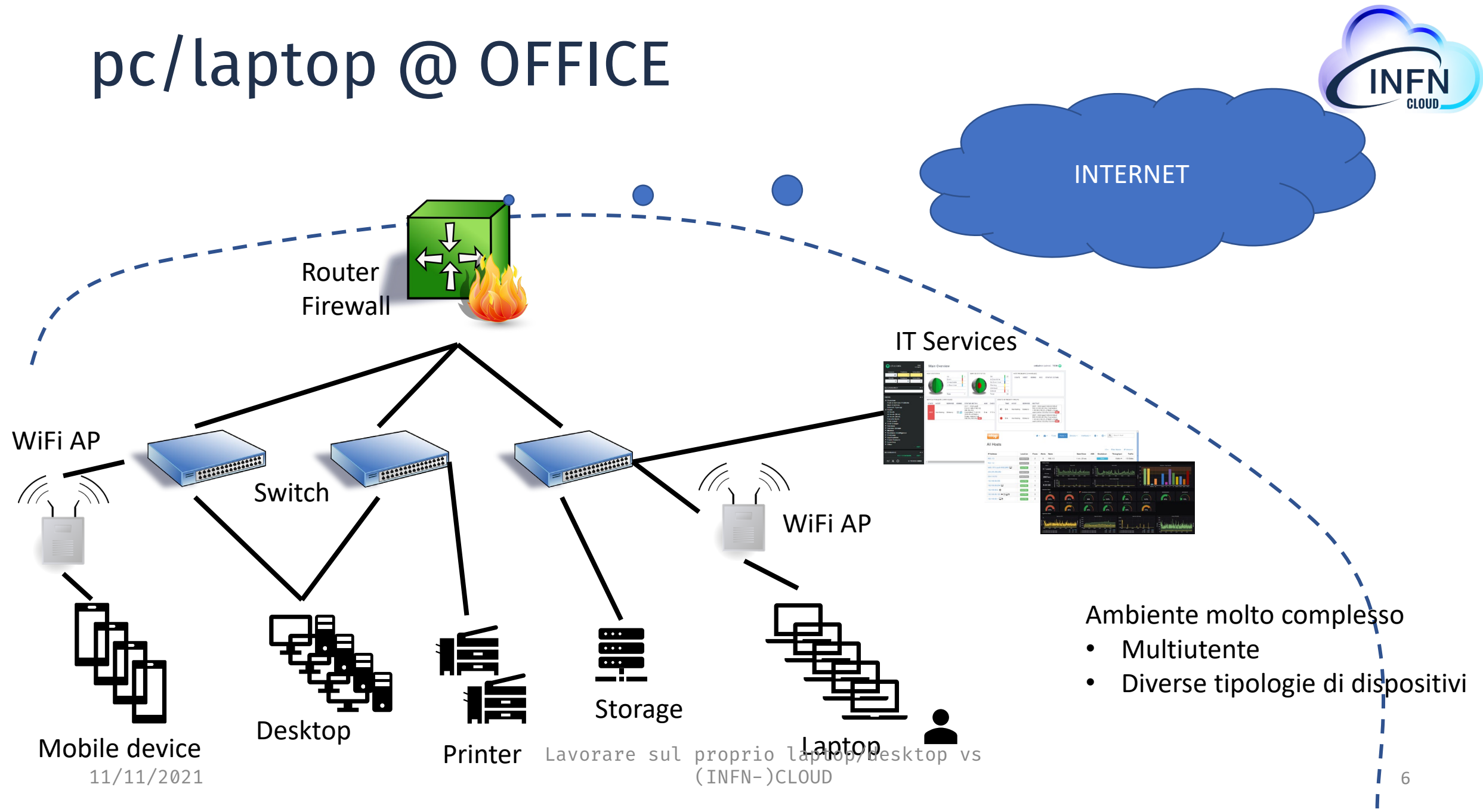
- Regole che permettono/inibiscono la comunicazione TRA oggetti all'interno rete privata (**gestite da voi**)
- Regole che permettono/inibiscono la comunicazione VERSO dispositivi della rete locale dall'esterno (**gestite da voi nell'ambito di quanto concesso dal provider**)
- Regole che permettono/inibiscono la comunicazione VERSO l'esterno dalla rete locale (**gestite da voi**)

Basate sul riconoscimento del dispositivo



- Regole che gli utenti sono tenuti a seguire per poter utilizzare la RETE del provider

pc/laptop @ OFFICE



Ambiente molto complesso

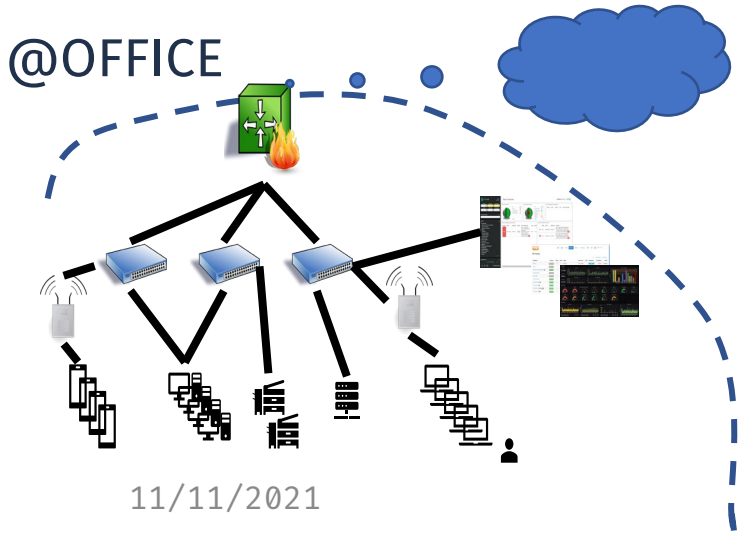
- Multiutente
- Diverse tipologie di dispositivi

@OFFICE: Policy locali e nazionali

- Regole che permettono/inibiscono la comunicazione TRA oggetti all'interno rete locale
- Regole che permettono/inibiscono la comunicazione VERSO dispositivi della rete locale dall'esterno
- Regole che permettono/inibiscono la comunicazione VERSO l'esterno dalla rete locale

Basate sul riconoscimento del dispositivo
Basate sul riconoscimento (ruolo) dell'utente

- Regole che gli utenti sono tenuti a seguire nell'utilizzo dei DISPOSITIVI loro assegnati
- Regole che gli utenti sono tenuti a seguire per poter utilizzare la RETE



- Se siete amministratori del vostro dispositivo, potete gestire un eventuale firewall presente sul vostro dispositivo
- In generale, dovete interfacciarvi con il vostro servizio calcolo locale per richiedere regole ad-hoc per un vostro dispositivo

Vale tutto quando esposto nella sessione del primo giorno: «Normativa di riferimento»

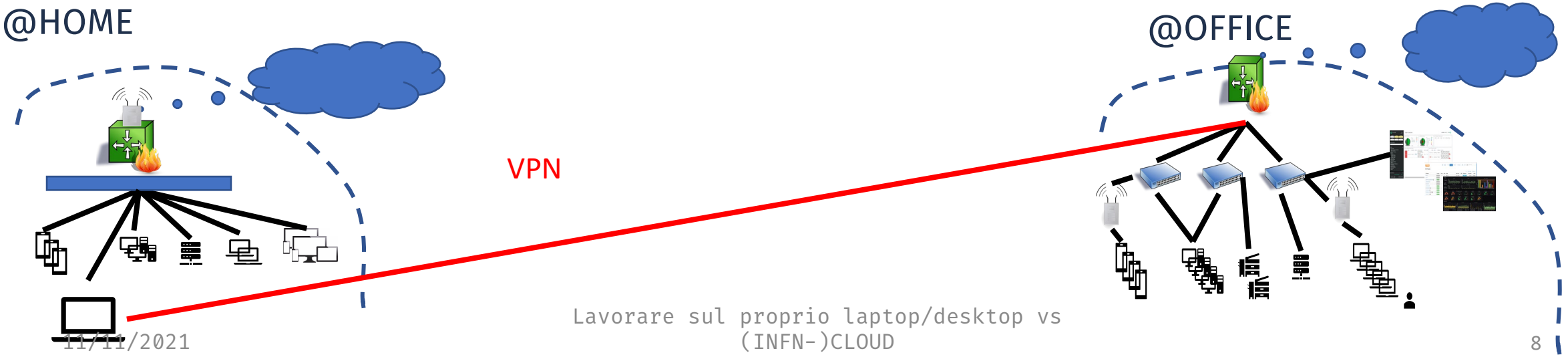
pc/laptop @ home + VPN

- La VPN crea un canale di rete virtuale verso la rete locale della vostra sezione
  - Il vostro dispositivo (e solo quello) è «*come se*» fosse presente nella rete locale della sezione e potete lavorare «*come se*» vi trovaste in ufficio
  - Allo stesso tempo, rimangono disponibili e accessibili i vostri dispositivi casalinghi

E’ importante che i dispositivi usati in ambito lavorativo non vengano usati anche per le attività personali

Tutti i dispositivi connessi alla VPN di sezione DEVONO essere configurati e gestiti in modo adeguato

- S.O. aggiornato
- Applicativi aggiornati
- Antivirus dell’INFN installato e aggiornato
- **Vale tutto quando esposto nella sessione del primo giorno: «Normativa di riferimento»**



Cluster di calcolo e servizi

- Un cluster di calcolo locale o un sito Grid, è un insieme di risorse (calcolo e storage) che viene utilizzato in modalità non privilegiata, ovvero come utenti.
  - Non è compito vostro amministrarlo
  - Non è compito vostro preoccuparvi del fatto che le risorse siano condivise con altri utenti
  - Non è compito vostro preoccuparvi della gestione dei dati degli utenti

- Queste considerazioni valgono in generale nell'utilizzo di tutti i servizi nei quali si è semplicemente utenti

- E' quello che in ambito Cloud chiameremo SaaS (Software as a Service)

- **Poiché non si hanno privilegi amministrativi e non si gestiscono dati personali, non viene richiesta un nomina di amministrazione di sistema in ambito cluster.**

Ripasso delle responsabilità di un utente di dispositivi TS (Tecnico Scientifici) in ambito INFN

- I sistemi detti **Tecnico Scientifici** sono quelli che hanno un solo utente (ad uso personale) e non trattano dati personali o considerati critici.
  - macchine per il calcolo single user
  - macchine per lo sviluppo
  - laptop e desktop personali, etc.

- In questo caso occorre rispettare il **disciplinare per l'uso delle risorse informatiche** ed impegnarsi ad applicare le buone pratiche consigliate da CCR che derivano dall' applicazione della direttiva AGID dette "**misure minime di sicurezza informatica**"

- Ovviamente occore rispettare tutte le leggi e I regolamenti esistenti di carattere generale, i termini delle **licenze d'uso** e la disciplina sulla violazione della proprieta' intellettuale. !! Leggiamo sempre cio' che accettiamo !!
  - Attenzione che molti applicativi concessi gratuitamente per uso personale, se li usiamo in ambito lavorativo siamo passibili di violazione di contratto d'uso

Vale tutto quando esposto nella sessione del primo giorno: «Normativa di riferimento»

Come funziona nei sistemi in cloud

In sezione i servizi calcolo tipicamente gestiscono:

- Un Firewall perimetrale che blocca il traffico non esplicitamente richiesto (e non è sotto il vostro controllo)
- Un sistema di Intrusion detection and prevention perimetrale che individua prontamente eventuali minacce (e non è sotto il vostro controllo)
- Un sistema antimalware che riduce il rischio di attacchi informatici (e non è sotto il vostro controllo)
- In generale vari sistemi di monitoraggio e allarmistica (e non sono sotto il vostro controllo)

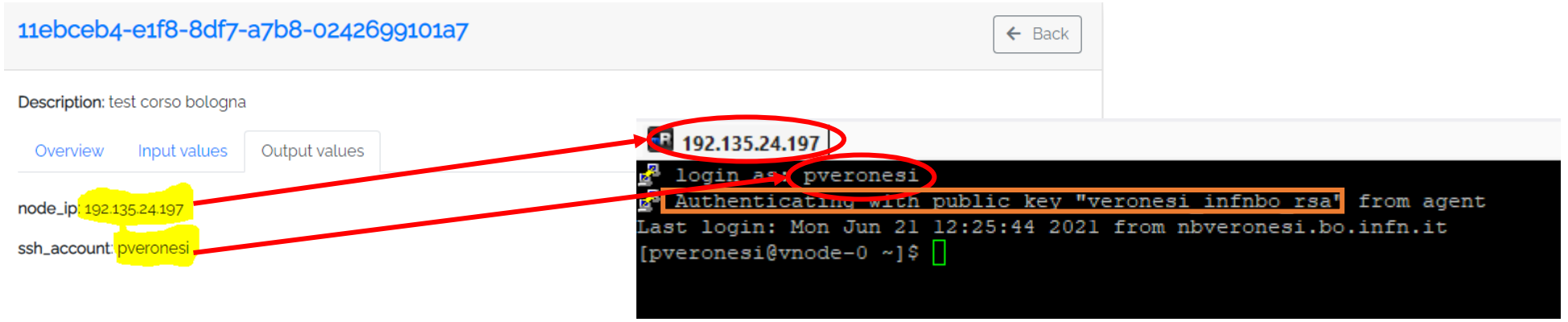
Sintettizzando, occorre la nomina di "amministratore di Sistema" quando:

- **Abbiamo un servizio esposto su rete pubblica**
- **Ci sono dati personali**

I servizi che create in ambito INFN Cloud sono sotto il vostro controllo (e responsabilità)

- I dispositivi di sicurezza sopra elencati tipicamente presenti in sezione non sono completamente disponibili nelle risorse di INFN Cloud o non sono disponibili i meccanismi per poterle gestire in autonomia (almeno per ora)
- Questo rende tali risorse, se non adeguatamente gestite, potenzialmente piu' vulnerabili ad attacchi informatici e al rischio data breach rispetto a medesimi servizi gestiti internamente alla sezione
- L'implementazione di tali servizi è (al momento) a carico degli utenti (che sono amministratori). Qualche dettaglio nei talk successivi

Es: Virtual Machine: Accesso e verifiche




```
[pveronesi@vnode-0 ~]$ df -mh
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        895M     0  895M   0% /dev
tmpfs           919M     0  919M   0% /dev/shm
tmpfs           919M   57M  863M   7% /run
tmpfs           919M     0  919M   0% /sys/fs/cgroup
/dev/vda1        10G  1.8G  8.3G  18% /
/dev/vdb1       8.8G   37M  8.3G   1% /data
tmpfs           184M     0  184M   0% /run/user/1001
[pveronesi@vnode-0 ~]$ cat /etc/redhat-release
CentOS Linux release 7.9.2009 (Core)
```

- Documentazione: https://guides.cloud.infn.it/docs/users-guides/en/latest/users_guides/getting_started.html#ssh-keys
- Quando si instanziano servizi nella PaaS di INFN Cloud, è sempre possibile accedere alla vm che ospita il servizio via ssh
- Come username si usa quello con cui viene visto l'utente
- NON è permessa la connession ssh con password, ma si accede solo via chiave che va precedentemente creata/aggiunta
  - Una volta che si è acceduto alla vm, è possibile eseguire operazioni di system administration via ***sudo***

Es: Virtual Machine: Aggiornare il S.O.

```
[pveronesi@vnode-0 ~]$ sudo yum check-update
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.digitalnova.at
 * epel: fedora.mirror.garr.it
 * extras: mirror.digitalnova.at
 * updates: mirror.digitalnova.at

bind-export-libs.x86_64
binutils.x86_64
ca-certificates.noarch
centos-release.x86_64
chkconfig.x86_64
cloud-init.x86_64
coreutils.x86_64
cpio.x86_64
curl.x86_64
hwdata.x86_64
kernel.x86_64
kernel-tools.x86_64
kernel-tools-libs.x86_64
kexec-tools.x86_64
kpartx.x86_64
krb5-libs.x86_64
libblkid.x86_64
libcroco.x86_64
libcurl.x86_64
libgcc.x86_64
libgomp.x86_64
libmount.x86_64
libpng.x86_64
libsmartcols.x86_64
libssh2.x86_64
libstdc++.x86_64
libteam.x86_64
libuuid.x86_64
libxml2.x86_64
libxml2-python.x86_64
lshw.x86_64
lz4.x86_64
mariadb-libs.x86_64
microcode_ctl.x86_64
openldap.x86_64
openssl.x86_64
openssl-libs.x86_64
teamd.x86_64
tuned.noarch
tzdata.noarch
util-linux.x86_64
vim-minimal.x86_64
wpa_supplicant.x86_64
xfsprogs.x86_64
zlib.x86_64
```

```
[pveronesi@vnode-0 ~]$ yum update -y kernel openssl
Loaded plugins: fastestmirror
You need to be root to perform this command.
[pveronesi@vnode-0 ~]$ sudo yum update -y kernel openssl
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.mirror.garr.it
 * epel: fedora.mirror.garr.it
 * extras: centos.mirror.garr.it
 * updates: centos.mirror.garr.it
Resolving Dependencies
--> Running transaction check
---> Package kernel.x86_64 0:3.10.0-1160.31.1.el7 will be installed
--> Processing Dependency: linux-firmware >= 20190429-72 for package: kernel-3.10.0-1160.31.1.el7.x86_64
---> Package openssl.x86_64 1:1.0.2k-19.el7 will be updated
---> Package openssl.x86_64 1:1.0.2k-21.el7_9 will be an update
--> Processing Dependency: openssl-libs(x86-64) = 1:1.0.2k-21.el7_9 for package: 1:openssl-1.0.2k-21.el7_9.x86_64
--> Running transaction check
---> Package linux-firmware.noarch 0:20200421-80.git78c0348.el7_9 will be installed
---> Package openssl-libs.x86_64 1:1.0.2k-19.el7 will be updated
---> Package openssl-libs.x86_64 1:1.0.2k-21.el7_9 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package                Arch          Version                    Repository  Size
================================================================================
Installing:
 kernel                 x86_64        3.10.0-1160.31.1.el7       updates     50 M
Updating:
 openssl                x86_64        1:1.0.2k-21.el7_9          updates    493 k
Installing for dependencies:
 linux-firmware         noarch        20200421-80.git78c0348.el7_9
                                                                  updates     80 M
Updating for dependencies:
 openssl-libs           x86_64        1:1.0.2k-21.el7_9          updates    1.2 M

Transaction Summary
================================================================================
```

In caso di aggiornamento del kernel, ricordarsi di fare il reboot

Es: Virtual Machine: Installazione web server

- Nel seguente esempio si procederà ad installare un web server (apache) e verificare l'accesso a tale servizio

- Installazione servizio (httpd e **mod_ssl**)

```
[pveronesi@vnode-0 ~]$ sudo yum install httpd mod_ssl -y
```

- Verifico lo stato delle porte http e https

```
[pveronesi@vnode-0 ~]$ sudo netstat -tunpl|egrep '80|443'
[pveronesi@vnode-0 ~]$
```

- Faccio partire il servizio e verifico ancora le porte http e https

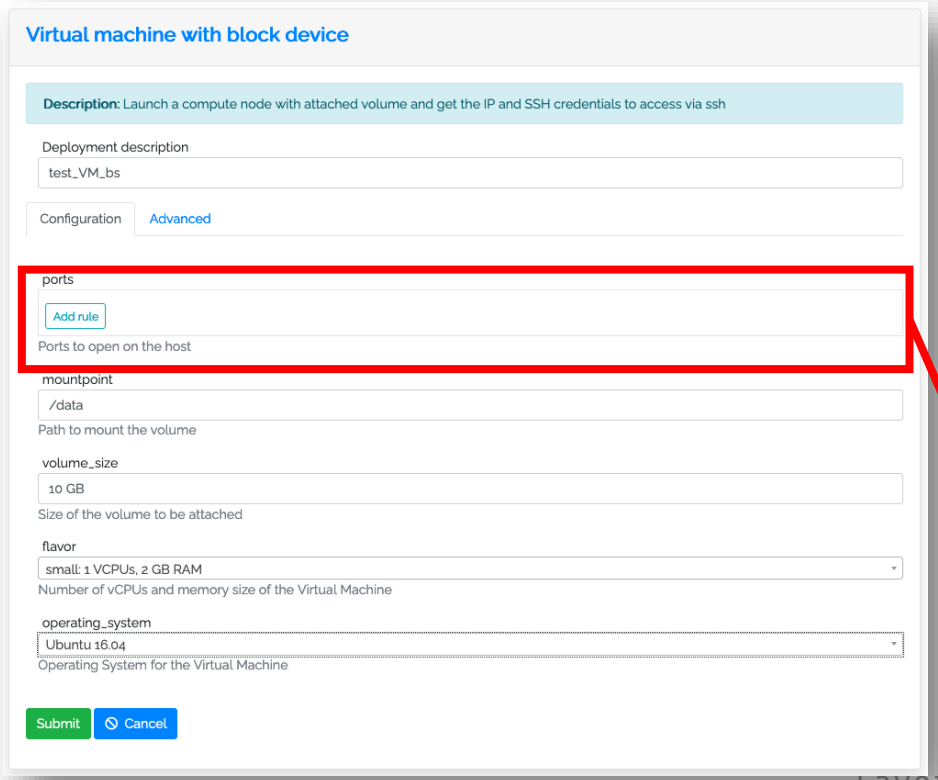
```
[pveronesi@vnode-0 ~]$ sudo systemctl start httpd
[pveronesi@vnode-0 ~]$ sudo netstat -tunpl|egrep '80|443'
tcp6       0      0 :::80                   :::*                    LISTEN      24528/httpd
tcp6       0      0 :::443                  :::*                    LISTEN      24528/httpd
```

Ma posso accedere al servizio? Controllo di tutta la catena

- **FW locale** (sotto il mio controllo)
- **Security group** (sotto il mio controllo parzialmente, vedi slide successiva)
- **FW di sezione** (sotto il controllo della sezione che ospita la vm).
  - In ambito INFN Cloud ci sono policy su quali porte devono essere aperte nel FW di sezione (talk successivi)

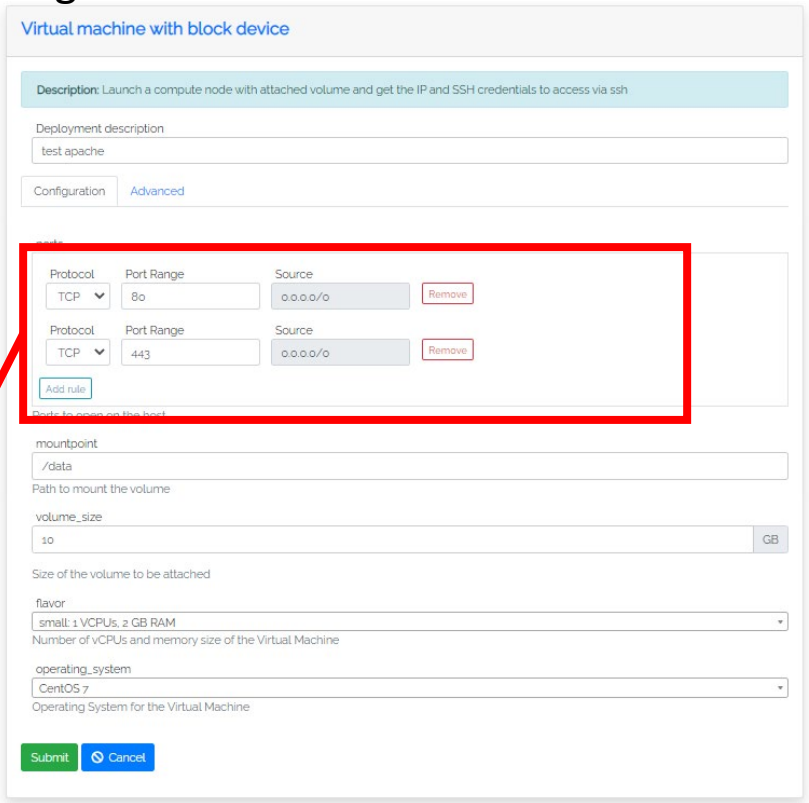
Es: Virtual Machine: Installazione web server Gestione apertura porte

- Al momento della creazione della vm, possiamo specificare un elenco di porte aggiuntive (oltre alla 22) che devono essere aperte
- Se la vm è già attiva, possiamo richiedere che venga aperta una porta specifica all'helpdesk https://servicedesk.cloud.infn.it/
- Analogamente è buona norma chiedere che una porta precedentemente aperta venga chiusa nel caso non sia usata



Ad oggi, in ogni deployment in INFN CLOUD, si ha almeno un IP su rete pubblica con almeno la porta 22 aperta (quindi) su Internet

Security Group (vedere talk successivo)



Es: Virtual Machine: Installazione web server apache - configurazione iniziale

```
<VirtualHost *:80>

        ServerName lnxpv.bo.infn.it

        ServerAdmin webmaster@bo.infn.it

        DocumentRoot /var/www/html/lnxpv

        ProxyRequests Off

        ErrorLog logs/lnxpv.bo.infn.it-error_log

        CustomLog logs/lnxpv.bo.infn.it-access_log combined

          RewriteEngine On

          RewriteCond %{HTTPS} off

          RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI}

</VirtualHost>
```

```
<VirtualHost *:443>
        ServerName lnxpv.bo.infn.it
        ServerAdmin webmaster@bo.infn.it
        DocumentRoot /var/www/html/lnxpv
        ProxyRequests Off

          SSLEngine On
          SSLProtocol -all +TLSv1.2 +TLSv1.3
          SSLHonorCipherOrder On
          SSLCipherSuite      ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-
POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-
AES256-SHA384:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256
          SSLCompression      off
          SSLSessionTickets   off

          SSLCertificateFile /etc/httpd/certs/lnxpv.crt
          SSLCertificateKeyFile /etc/httpd/certs/lnxpv.key
          SSLCertificateChainFile /etc/httpd/certs/intermediate.crt

        CustomLog logs/lnxpv.bo.infn.it-access_log combined
        CustomLog logs/lnxpv.bo.infn.it-ssl_request_log ssl_request_client_cn
        ErrorLog logs/lnxpv.bo.infn.it-error_log

</VirtualHost>
```

```
# firewall-cmd --zone=public --add-service=http --permanent
# firewall-cmd --zone=public --add-service=https --permanent
# firewall-cmd --reload
```

Da considerarsi best practice e quindi soggette a continue variazioni e aggiornamenti

Lavorare sul proprio laptop/desktop vs (INFN-)CLOUD

Riassumendo

- Security first: sia in qualità di utenti che a maggior ragione se gestiamo servizi, la sicurezza informatica deve essere al centro della nostra attività
  - Non è solo un obbligo di legge
- Conoscere l'ambiente nel quale siamo inseriti come utenti e/o nel quale opererà un servizio che forniamo è fondamentale
  - Attenzione ai figli che usano il pc a casa con il quale ogni tanto ci colleghiamo in VPN all'ufficio
  - In ufficio/Cloud non condividete account generici o credenziali per fare prima
  - Qualche nozione sul networking per forza dovete acquisirla
- Conoscere gli applicativi su cui si basa il servizio che gestiamo
  - Features
  - Best practice (install&start non è una best practice!)
  - Release Notes quando aggiorniamo, …
- La risposta è: **SI**
  - Tutto questo porta via del tempo
  - può complicare un'attività che ci sembrava semplice
  - Può stravolgere un prototipo che era già pronto per essere messo in produzione

- **C'e il SUPPORTO, usatelo anche per pianificare prima sulla carta la vostra idea**
  - Calcolo e Reti della vostra sezione
  - INFN Cloud servicedesk
  - Security Group INFN
  - Richiedete di frequentare corsi per «amministratori di sistema» al vostro referente della formazione locale