Sicurezza e rischio informatico su INFN Cloud

Setup di rete in INFN Cloud

Gianluca Peco, Stefano Stalio, Paolo Veronesi

Sommario

- Architettura di rete
- Limitazione e controllo dell’accesso ai servizi
- DNS e certificati x509, servizi basati su http
- Incidenti più comuni

Risorse virtuali e rete

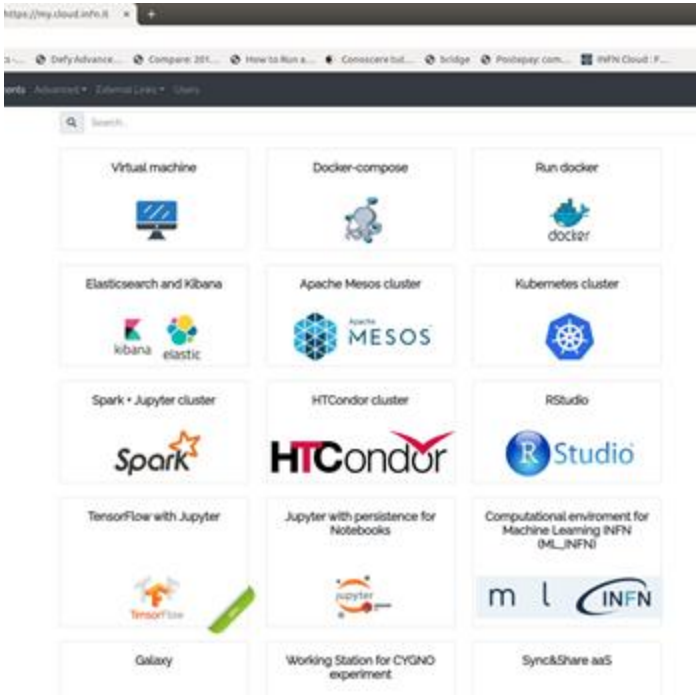
L'interazione con dei servizi Cloud implica generalmente un qualche tipo di accesso a virtual host (VM) collegati in rete.

Solitamente le VM in questione risiedono in una rete privata assieme ad altre VM. Ad esempio perché assieme contribuiscono ad offrire un servizio, o perché sono gestite dallo stesso progetto

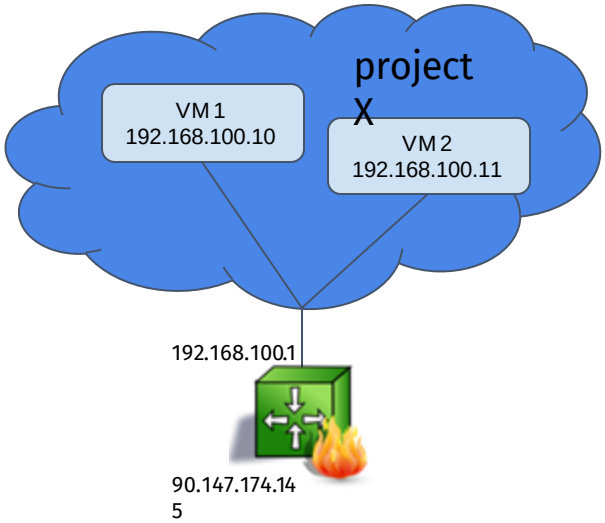
Una cloud ospita generalmente più reti private. Le reti private separano gruppi di VM che per qualche motivo devono/possono comunicare tra loro da altri.

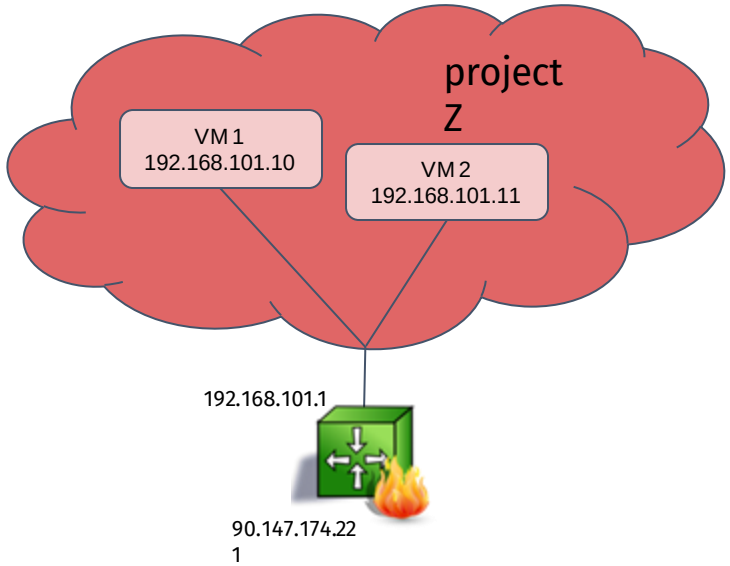
Reti private diverse non sono generalmente interconnesse.

All'interno della rete privata solitamente funziona un servizio DNS interno che permette sia la risoluzione diretta dei nomi delle VM in indirizzi IP che quella inversa da indirizzo IP in nome.



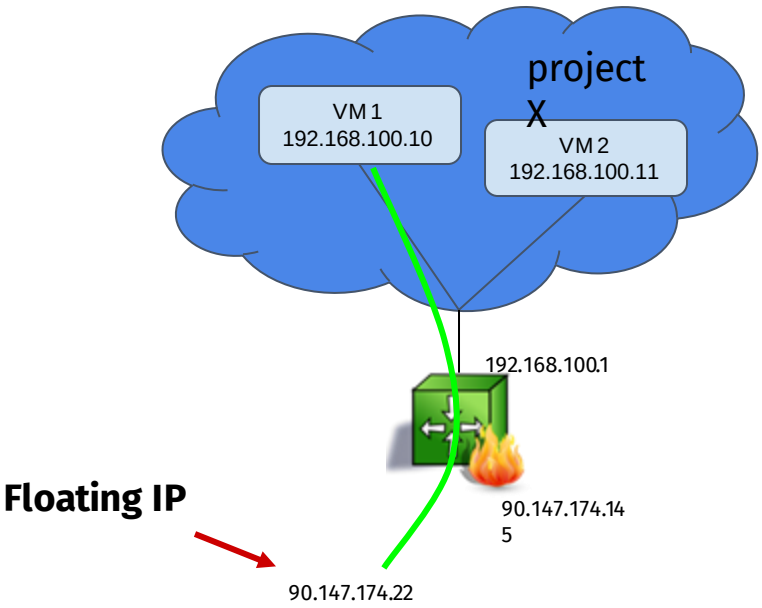
La rete di progetto… vista dall'utente





La configurazione della rete di un progetto su INFN Cloud è molto simile a quella della rete di casa. Risorse istanziate su progetti diversi sono completamente isolate tra loro.

I Floating IP

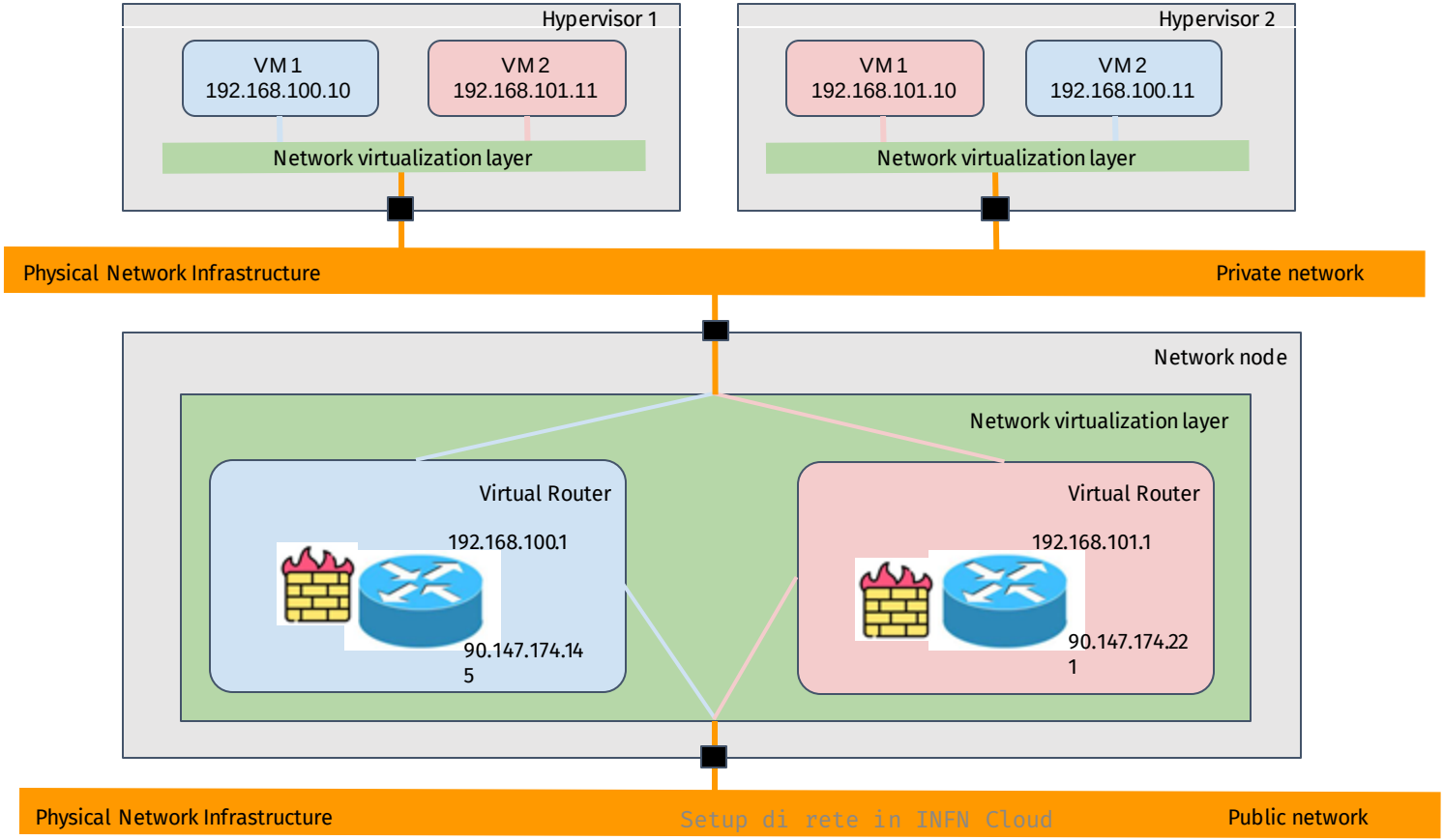


I floating IP sono un mezzo per dare accesso dall'esterno della cloud ai servizi istanziati sulla cloud stessa.

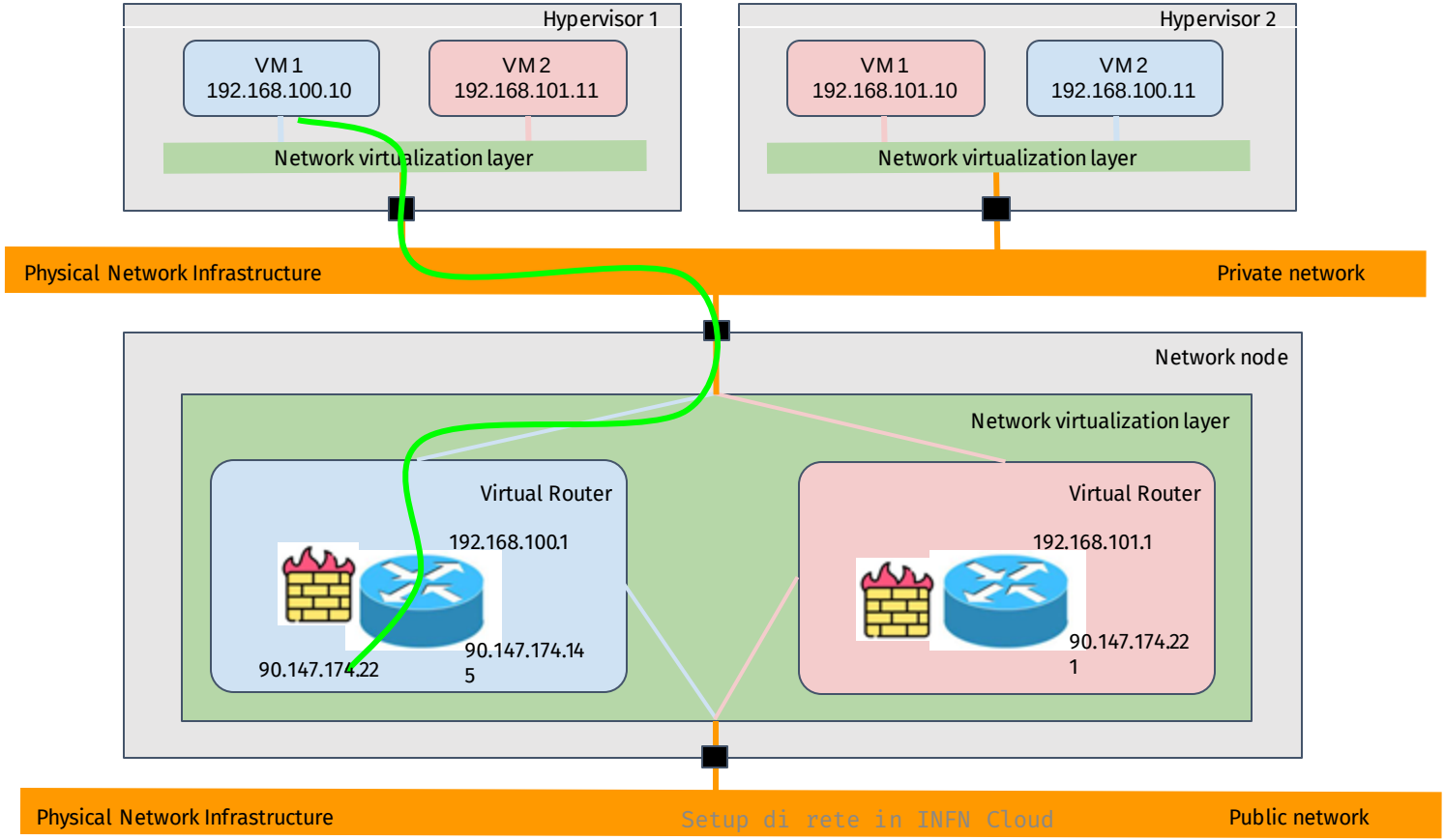
Non tutte le cloud, e non tutte le cloud federate ad INFN Cloud, usano questa tecnologia, alcune infrastrutture usano strumenti diversi per ottenere lo stesso scopo.

L'architettura qui descritta è però quella più comunemente usata

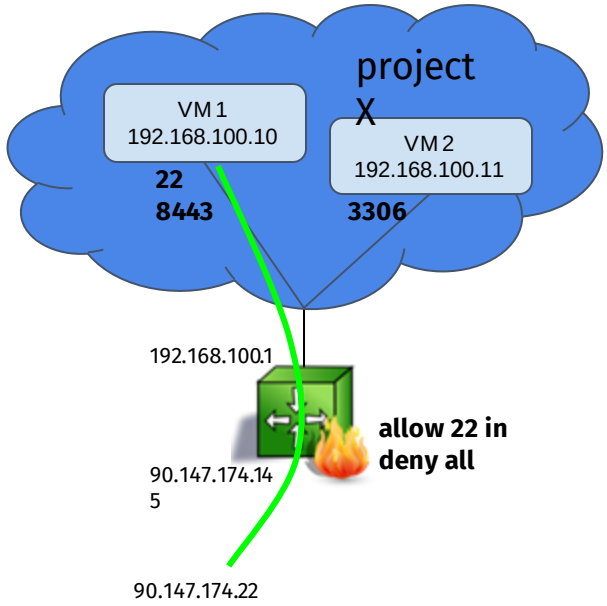
La rete di progetto... layout fisico



La rete di progetto... layout fisico



I Security Group



I security group sono insiemi di regole che permettono di controllare l'accesso ai servizi esposti dalle VM in esecuzione sulla cloud

Sono "regole di firewall" che vengono applicate sulle VM stesse

*A security group is **a named collection of network access rules that are used to limit the types of traffic that have access to instances**. When you launch an instance, you can assign one or more security groups to it.*

https://docs.openstack.org/

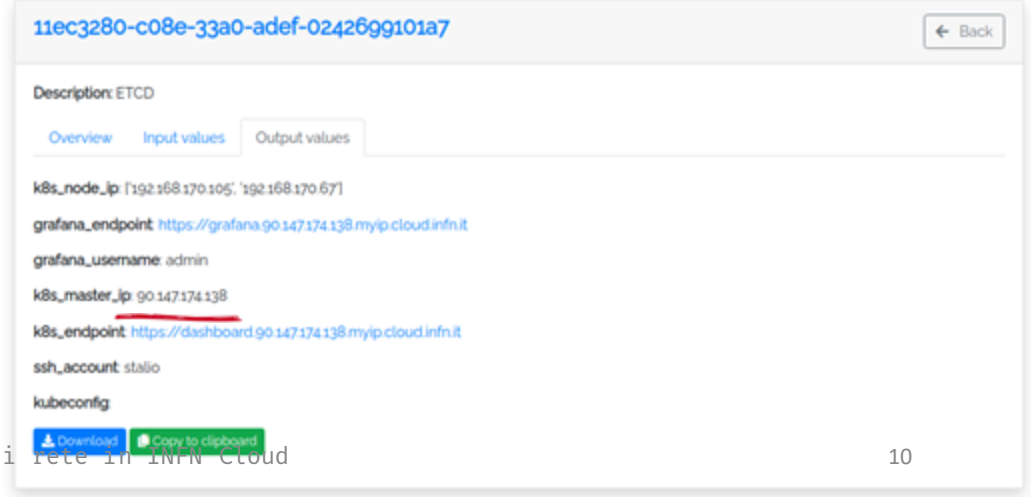
Regole per l’accesso remoto

In linea generale su una IaaS quando un Floating IP viene associato ad una VM le regole di accesso iniziali sono molto stringenti: **nessun accesso**

L’utente, **con una azione conscia e responsabile**, decide quali servizi renderà disponibili ed attraverso quali porte

Accesso remoto su INFN Cloud

- ogni servizio che viene creato su INFN Cloud via PaaS ha un indirizzo IP pubblico che espone almeno la porta 22 (ssh)
- chi ha creato il servizio può usare ssh per l'accesso alla/alle VM che lo ospitano



Controllo sui parametri di accesso remoto

Per ogni servizio istanziabile dagli utenti, dove tali parametri non siano già predefiniti, INFN Cloud da all'utente uno strumento per decidere quali porte esporre.

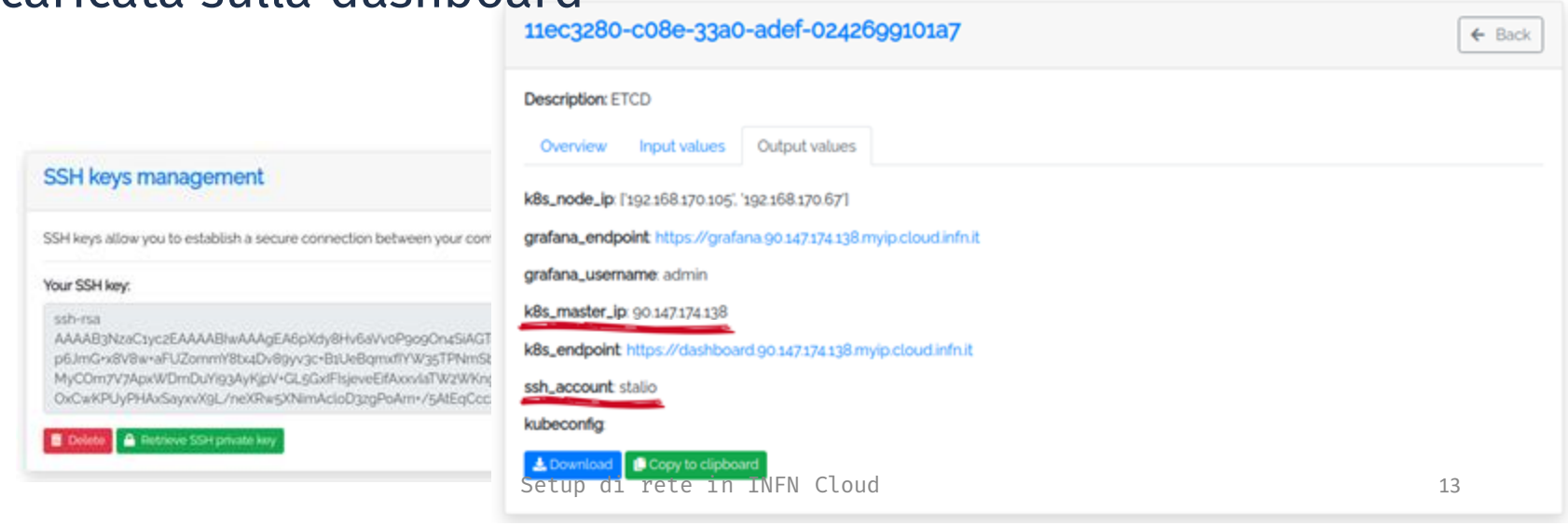
Controllo sui parametri di accesso remoto

Al momento l'unico modo per modificare la configurazione delle regole per l'accesso remoto (= porte aperte) dopo che un servizio è già attivo è aprire un ticket su https://servicedesk.cloud.infn.it

In futuro l'utente finale potrebbe essere autonomo per questa operazione

Accesso SSH

- L'accesso SSH avviene con la stessa username con cui l'utente è registrato nello IAM di INFN Cloud, per gli utenti INFN la username AAI, e con la chiave ssh caricata sulla dashboard



Accesso a VM senza IP pubblico

- se il servizio usa più VM, le macchine virtuali che non hanno un indirizzo IP pubblico possono essere accedute attraverso quella che lo espone.

Usando la VM con IP pubblico come jump host

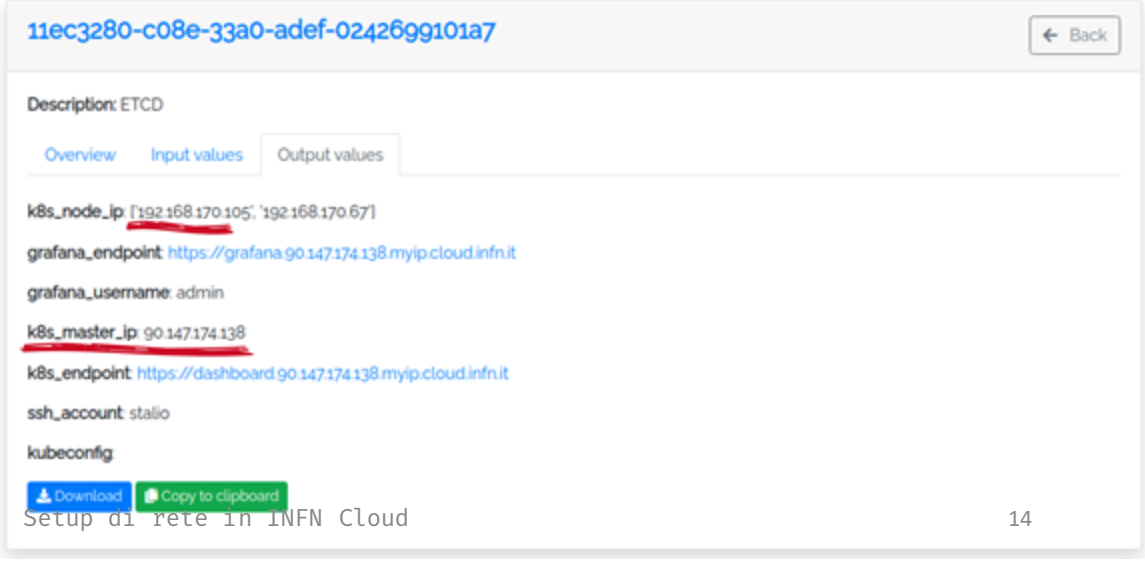
ssh 192.168.170.105 -J 90.147.174.138

Oppure accedendo prima alla macchina con ip pubblico

ssh -A 90.147.174.138

e da lì a quella interna

ssh 192.168.170.105

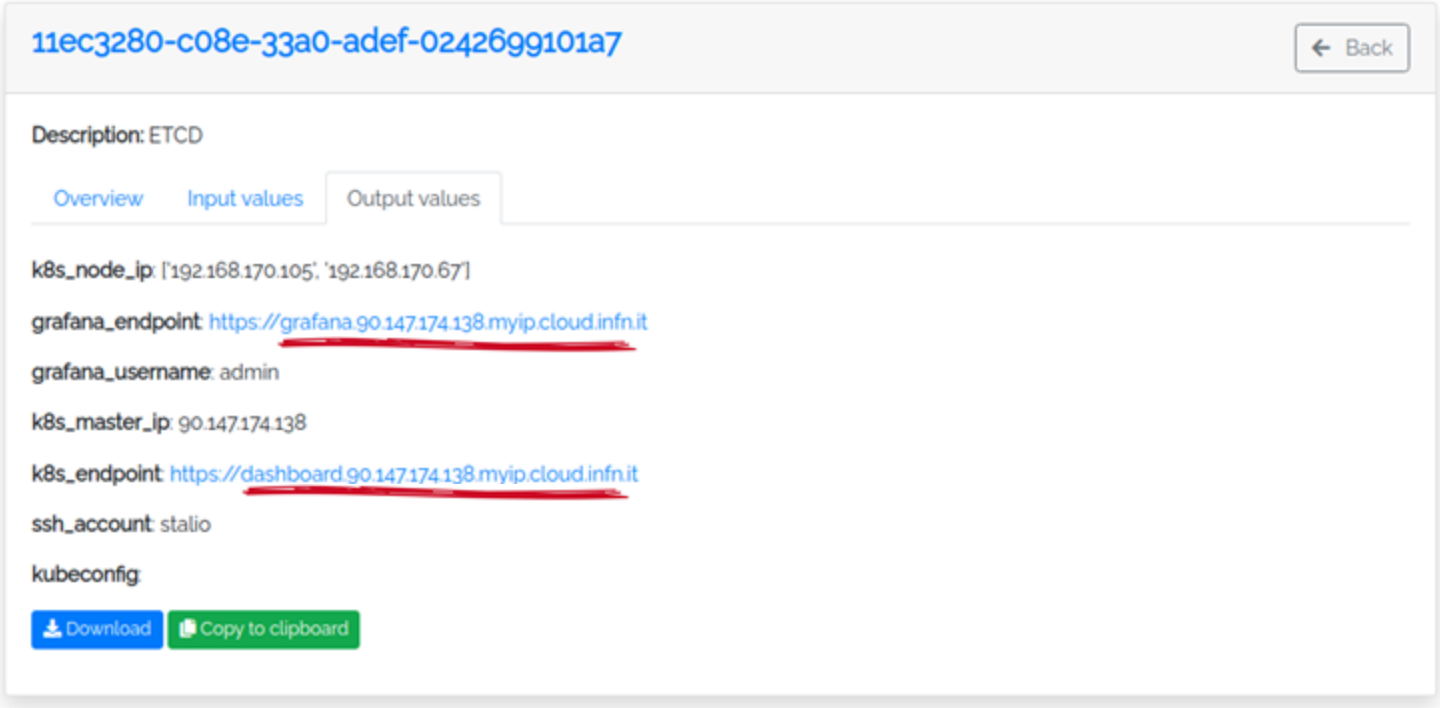


Servizio wildcard DNS

- INFN Cloud usa un meccanismo di wildcard DNS introdotto da xip.io (servizio ora non più attivo) e ripreso poi da https://nip.io/ e da altri.
- ogni indirizzo pubblico di INFN Cloud, es. 90.147.174.138, è automaticamente risolto da qualsiasi hostname nelle forme seguenti:
  - 90.147.174.138.myip.cloud.infn.it
  - <nome>.90.147.174.138.myip.cloud.infn.it
  - <nome>.<nome>.90.147.174.138.myip.cloud.infn.it

  e così via

Servizio wildcard DNS



Servizio DNS di INFN Cloud

I progetti che usano risorse INFN Cloud possono chiedere che agli indirizzi IP pubblici usati dai servizi che hanno istanziato siano assegnati dei nomi DNS, nella forma

<nome>.<progetto>.cloud.infn.it

Ad esempio:

wiki.herd.cloud.infn.it

Servizio DNS di INFN Cloud

- I progetti che usano risorse INFN Cloud possono chiedere che ad ogni indirizzo IP pubblico usato dai servizi che hanno istanziato sia assegnato anche **più di un nome DNS**

- Il servizio DNS di INFN Cloud fornisce la traduzione diretta, da nome ad indirizzo, ma non quella inversa da indirizzo a nome

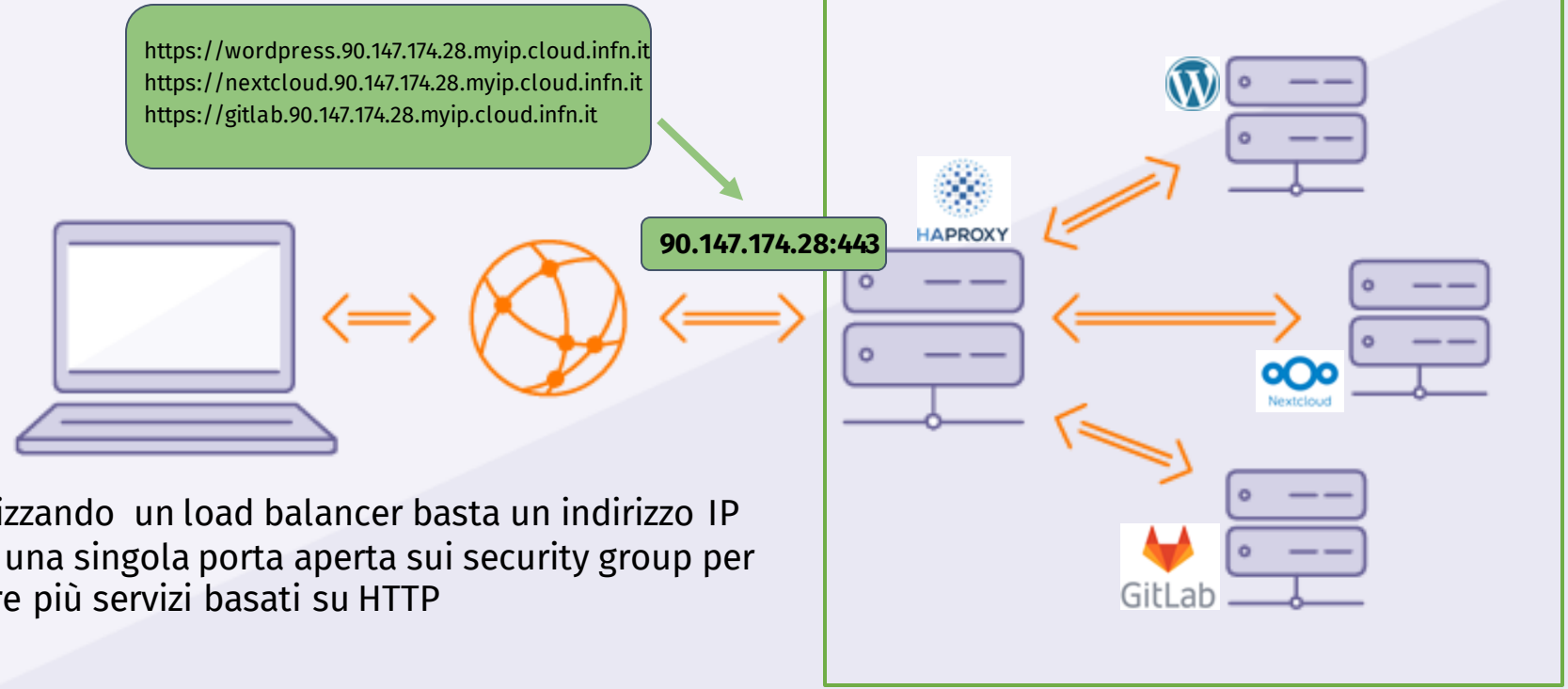
- Oggi tali richieste devono essere fatte attraverso un ticket su https://servidesk.cloud.infn.it

In futuro il servizio potrebbe evolvere rendendo i progetti autonomi nel gestire i nomi all'interno del proprio sottodominio e la loro associazione agli indirizzi pubblici usati dai servizi istanziati dal progetto stesso

Importanza del DNS per la sicurezza

- L’esistenza di nomi DNS legati agli IP pubblici delle VM istanziate su INFN Cloud rende possibile la richiesta di certificati server x509 per la criptazione delle connessione con SSL
- possono essere certificati Let’s Encrypt, ottenibili autonomamente dall’utente e per i quali è possibile definire procedure di rinnovo automatico
- possono essere certificati ottenuti gratuitamente grazie al servizio offerto dal GARR attraverso gli RAO di INFN Cloud, facendo richiesta su https://servicedesk.cloud.infn.it

Importanza del DNS per la sicurezza



Utilizzando un load balancer basta un indirizzo IP con una singola porta aperta sui security group per offire più servizi basati su HTTP

Importanza del DNS per la sicurezza

- Solo connessioni sicure
- Poche porte esposte
- Singolo punto di accesso

Maggiore sicurezza

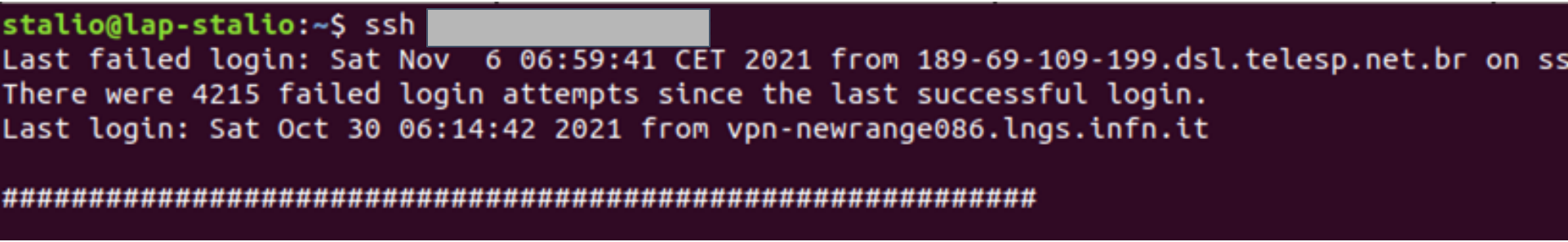
Incidenti più comuni

- Accesso ssh tramite attacchi di tipo “brute force”
- Accesso ad applicazioni protette da password banali
- Web site defacement

SSH - brute force password discovery

- I servizi SSH sono sotto continuo attacco con tentativi di accesso basati su dizionari di username e password
- L’utilizzo di chiavi SSH anziché password elimina il rischio dovuto a questo tipo di attacco (ovviamente è fondamentale proteggere le proprie chiavi provate)
- Se l’uso della password è necessario, è necessario anche adottare ulteriori misure di protezione

SSH - brute force password discovery



Web site defacement

- Dove l'accesso via password è inevitabile,

  NON USARE USERNAME E PASSWORD BANALI

- Uno dei rischi dell'utilizzo di username/password comuni e il defacement di un sito web
- Ma il defacement di un sito web può anche avere origine da accessi non autorizzati resi possibili da vulnerabilità in plugin di terze parti in esecuzione sul sito compromesso da vulnerabilità dell'applicazione stessa

Website defacement is an attack on a website that changes the visual appearance of a website or a web page.

https://en.wikipedia.org/wiki/Website_defacement

Web site defacement