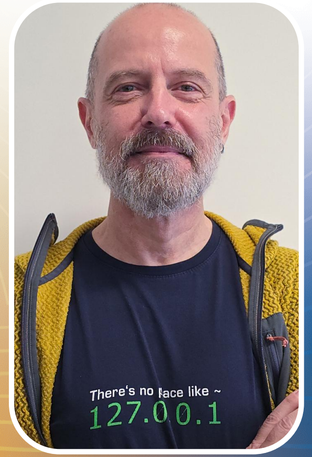
WORKSHOP GARR 2026

NET MAKERS

Sostenibilità e governance del data centre ISTI



Andrea Dell'Amico

CNR-ISTI · D4Science

Consiglio Nazionale delle Ricerche · Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo" · D4SCIENCE INFRASTRUCTURE

2026-11-02

Sostenibilità e governance del data centre ISTI



(20 s) Mi presento: gestisco l'infrastruttura di calcolo di D4Science all'ISTI. Racconto come stiamo costruendo il nuovo data center, soprattutto come ne automatizziamo la gestione, e come pianifichiamo la vita dell'hardware.

Workshop GARR 2025: la connettività

Workshop GARR 2025 · 3 novembre

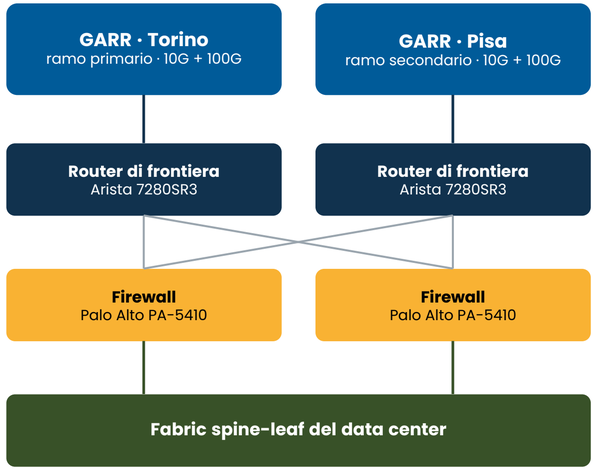
CNR: un esempio di standardizzazione per le infrastrutture di rete

Ermann Ripepi (CNR-IMAA), Andrea Dell'Amico (CNR-ISTI)

Connettività del nuovo data center, IP fabric, accesso alla rete GARR

Presentazione e video
nell'archivio del Workshop 2025

ws25.garr.it/it/speaker/andrea-dellamico





(1 min) Al Workshop dell'anno scorso, con Ermann Ripepi del CNR-IMAA, abbiamo presentato la connettività del nuovo data center e il modello di IP fabric condiviso fra i due istituti. Presentazione e video sono nell'archivio del Workshop 2025, raggiungibili dal link o dal QR code. In sintesi: due rami GARR indipendenti, primario verso Torino e secondario verso Pisa, ciascuno con 10 Gb/s di Internet e 100 Gb/s dedicati; due router di frontiera Arista e due firewall Palo Alto. Oggi mi concentro su come configuriamo e gestiamo l'infrastruttura.

1. L’infrastruttura in breve

Rete, calcolo, storage, indirizzamento, governance

WORKSHOP GARR 2026

NET MAKERS

(5 s) Prima parte, breve: i componenti del nuovo data center.

Componenti del nuovo data center

Rete

IP fabric spine-leaf con EVPN/VXLAN (Underlay BGP)

BGP fino all'host con FRR e BFD

3 availability zone, una per coppia di leaf

Calcolo

Circa 75 server

Nodi iperconvergenti per calcolo e storage Ceph

Nodi GPU con A100 e H100

Cloud e storage

OpenStack 2026.2 con Kolla-Ansible e OVN

Ceph con cephadm, replica 3

Proxmox per i servizi di base: DNS, resolver, autenticazione, VPN

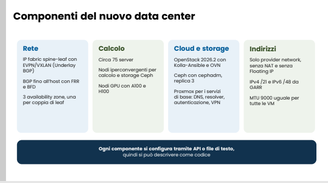
Indirizzi

Solo provider network, senza NAT e senza Floating IP

IPv4 /21 e IPv6 /48 da GARR

MTU 9000 uguale per tutte le VM

Ogni componente si configura tramite API o file di testo,
quindi si può descrivere come codice



(1 min 30 s) La rete è un IP fabric spine-leaf su switch Arista, con EVPN/VXLAN e underlay BGP; i server scambiano rotte BGP con i leaf tramite FRR, e ogni coppia di leaf forma un'availability zone. I server sono circa 75: nodi iperconvergenti che svolgono sia il calcolo sia lo storage Ceph, nodi GPU e server per i servizi di base. OpenStack 2026.2 è installato con Kolla-Ansible e usa OVN; Ceph è installato con cephadm. I servizi di base, cioè DNS, resolver, autenticazione, VPN, backup e monitoraggio, girano su Proxmox, separati dal cloud. Ogni VM riceve un indirizzo diretto, senza NAT. Tutti questi componenti si configurano tramite API o file di testo, e questo rende possibile un'automazione completa. Se qualcuno chiede: abbiamo valutato anche L2/LACP con MLAG e reti tenant con Floating IP.

Governance del data center

in definizione

Gestione

Scelte tecniche sull'infrastruttura comune

Priorità degli interventi

Crescita

Capacità di calcolo, storage e rete

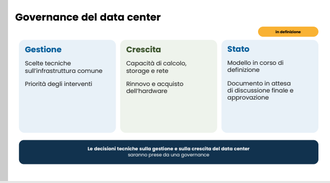
Rinnovo e acquisto dell'hardware

Stato

Modello in corso di definizione

Documento in attesa di discussione finale e approvazione

Le decisioni tecniche sulla gestione e sulla crescita del data center
saranno prese da una governance



(40 s) Le decisioni tecniche sulla gestione e sulla crescita del data center saranno prese da una governance: le scelte sull'infrastruttura comune, le priorità degli interventi, la capacità e il rinnovo dell'hardware. Il modello è in corso di definizione e la bozza del documento non è ancora approvata, quindi oggi non entro nei dettagli.

2. Automazione

Ogni aspetto delle configurazioni è gestito come codice, revisionato e versionato

WORKSHOP GARR 2026

NET MAKERS

2. Automazione

Ogni aspetto delle configurazioni è gestito come codice, revisionato e versionato

(5 s) Seconda parte, la principale: la configurazione e la gestione automatica.

Le ragioni dell’automazione

1. **Un gruppo piccolo**
   Le stesse persone gestiscono rete, cloud, storage e servizi

2. **Riproducibilità**
   L’infrastruttura deve essere completamente ricostruibile a partire da codice e inventario. I backup coprono la disponibilità dei dati e non le configurazioni attive sui sistemi, a meno che non sia indispensabile

3. **Tracciabilità**
   Ogni modifica deve essere associabile a un commit su Git e possibilmente avere superato una review

4. **Continuità delle conoscenze**
   Il codice documenta le scelte anche quando le persone cambiano

Codice già in uso per D4Science

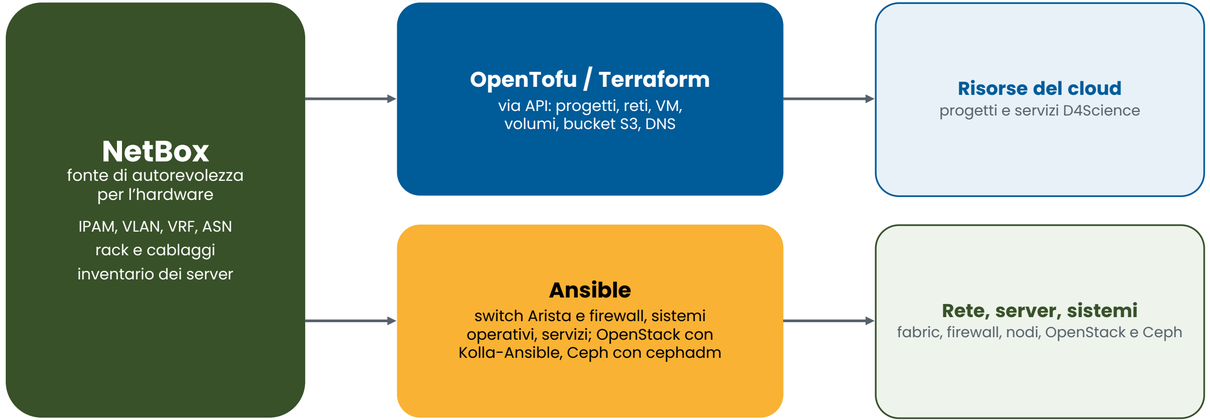
52 unità Terragrunt	**60** moduli OpenTofu
306 VM dichiarate	**281** volumi Cinder
254 security group	**105** ruoli Ansible

Cloud CNR-ISTI e regioni GARR CT1, NA, PA1

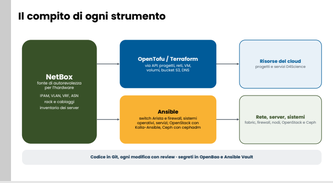


(1 min 30 s) Il gruppo è piccolo e le stesse persone gestiscono rete, cloud, storage e servizi. L’infrastruttura deve poter essere ricostruita completamente a partire da codice e inventario: i backup servono a garantire la disponibilità dei dati, e includono le configurazioni attive sui sistemi solo quando è indispensabile. Ogni modifica deve corrispondere a un commit in Git e, quando possibile, passare da una review. Il codice conserva le conoscenze anche quando le persone cambiano. Gli ambienti D4Science attuali, sul cloud ISTI e sulle regioni GARR, sono già descritti in OpenTofu, e i servizi si installano con oltre cento ruoli Ansible. I numeri a destra contano le risorse dichiarate nel codice. Nel nuovo data center estendiamo lo stesso metodo alla rete e ai server fisici.

Il compito di ogni strumento

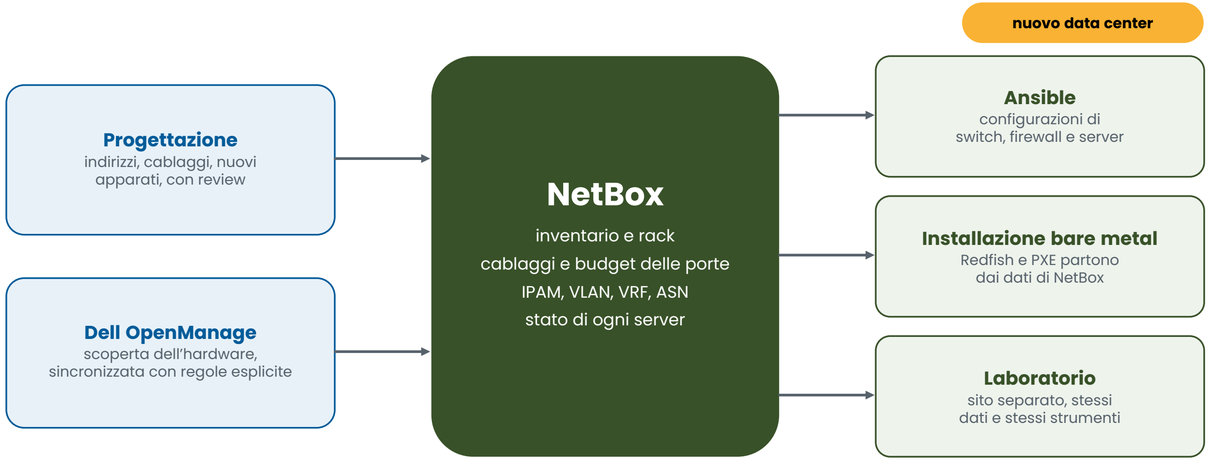


Codice in Git, ogni modifica con review · segreti in OpenBao e Ansible Vault

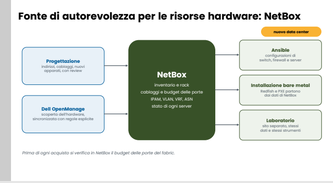


(1 min 30 s) Ogni strumento ha un compito preciso. NetBox è la fonte di autorevolezza per l'hardware: indirizzi, VLAN, VRF, ASN, rack e cablaggi. OpenTofu, o Terraform, configura tramite API le risorse del cloud: progetti, reti, VM, volumi, bucket S3, record DNS. Ansible configura sistemi operativi e servizi, installa OpenStack con Kolla-Ansible e Ceph con cephadm, e configura anche gli switch Arista e i firewall a partire dai dati di NetBox. Il codice sta in Git e ogni modifica passa da una review; i segreti stanno in OpenBao e in Ansible Vault.

Fonte di autorevolezza per le risorse hardware: NetBox



Prima di ogni acquisto si verifica in NetBox il budget delle porte del fabric.



(1 min 15 s) Nel nuovo data center NetBox descrive le risorse hardware: inventario, rack, cablaggi, indirizzi, VLAN, VRF, ASN e stato di ogni server. Istanze e risorse virtuali sono descritte nel codice OpenTofu. I dati entrano in NetBox dalla progettazione, con le stesse review del codice, e dalla scoperta automatica di Dell OpenManage Enterprise, che sincronizza secondo regole esplicite. Ansible, la pipeline di installazione dei server e il laboratorio leggono da NetBox; il laboratorio è un sito separato con gli stessi strumenti. In NetBox teniamo anche il budget delle porte del fabric, che controlliamo prima di ogni acquisto.

Configurazione automatica della rete

nuovo data center

1 — Dati
NetBox: interfacce, indirizzi, ASN, VLAN

→

2 — Template
Ansible genera le configurazioni EOS, FastIron, PAN-OS

→

3 — Review
pull request con il diff rispetto all'esercizio

→

4 — Laboratorio
fabric isolato: 2 spine, 4 leaf

→

5 — Produzione
controlli prima e dopo l'applicazione

Apparati

- Arista: spine, leaf e router di frontiera
- Palo Alto PA-5410, Brocade ICX per la gestione fuori banda

Regole

- Piano di rollback per ogni modifica di routing o firewall
- Backup automatico della configurazione dopo ogni modifica



(1 min 30 s) Ansible legge da NetBox interfacce, indirizzi, ASN e VLAN e genera da template le configurazioni per Arista EOS, per i Brocade della rete di gestione e per i firewall Palo Alto. La configurazione generata si rivede in una pull request, insieme al diff rispetto a quella in esercizio. Le modifiche si provano su un fabric di laboratorio isolato e poi si applicano in produzione, con controlli prima e dopo. Ogni modifica di routing o firewall richiede un piano di rollback, e dopo ogni modifica la configurazione degli apparati viene salvata automaticamente.

Dal server nuovo al nodo in servizio

nuovo data center

1 — Registrazione
il server entra in NetBox con rack e cablaggi

2 — Redfish
BMC configurato e verificato da remoto

3 — Installazione
PXE con Bifrost o Kayobe

4 — Baseline
Ansible: utenti, rete, FRR, monitoraggio

5 — Ruolo
Kolla-Ansible per OpenStack, cephadm per Ceph

6 — Collaudo
test automatici, stato aggiornato in NetBox

Primo passo
Inventario completo in NetBox, poi prova di Bifrost, Kayobe e Redfish su un nodo per ogni famiglia di server.



(1 min 15 s) Anche l'installazione dei server fisici segue una pipeline. Il server viene registrato in NetBox con rack e cablaggi; il BMC, iDRAC per i Dell, si configura e si verifica via Redfish; il sistema operativo si installa via PXE con Bifrost o Kayobe, oppure con il virtual media di Redfish. Ansible applica la configurazione di base: utenti, rete, FRR, monitoraggio. Segue il ruolo: Kolla-Ansible per OpenStack, cephadm per Ceph. Un collaudo automatico chiude il processo e aggiorna lo stato del server in NetBox. Cominciamo con un nodo per ogni famiglia di hardware.

Gestione del cloud con OpenTofu e Terragrunt

in uso oggi

Moduli OpenTofu
VM, reti, security group, DNS, volumi, share Manila, bucket S3, bilanciatori, Kubernetes

↓

Configurazione comune
un modulo per ogni tipo di servizio

↓

Unità Terragrunt
una per servizio e progetto, ciascuna con il proprio stato

Le capacità di ogni cloud (CNR, GARR) sono dichiarate per regione

Transizione a Terragrunt in corso di completamento

– Stessa struttura per tutti gli ambienti, sul cloud CNR e sulle regioni GARR

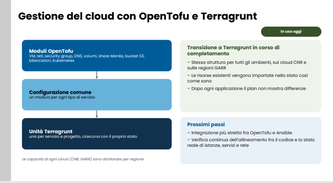
– Le risorse esistenti vengono importate nello stato così come sono

– Dopo ogni applicazione il plan non mostra differenze

Prossimi passi

– Integrazione più stretta fra OpenTofu e Ansible

– Verifica continua dell'allineamento fra il codice e lo stato reale di istanze, servizi e rete



(2 min) Questa parte è già in uso. Il codice ha tre livelli: i moduli OpenTofu descrivono i tipi di risorsa, una configurazione comune li adatta a ciascun tipo di servizio, e le unità Terragrunt, una per servizio e progetto, hanno ciascuna il proprio stato. Le capacità di ogni cloud sono dichiarate per regione, quindi gli stessi moduli funzionano sul cloud CNR, con Octavia OVN, Manila e Designate, e sulle regioni GARR. È in corso di completamento la transizione di tutti gli ambienti a Terragrunt, per gestirli in modo uniforme; le risorse esistenti vengono importate nello stato così come sono. I prossimi passi: un'integrazione più stretta fra OpenTofu e Ansible, e controlli continui che verifichino l'allineamento fra il codice e lo stato reale di istanze, servizi e configurazioni di rete.

3. Sostenibilità dell’hardware

Rinnovo e crescita pianificati dall’inizio

WORKSHOP GARR 2026

NET MAKERS

(5 s) Terza parte: la pianificazione dell’hardware nel tempo.

Un piano di rinnovo e di crescita

Progetti europei

D4Science partecipa da parecchi anni a progetti europei e prevede l'allocazione di una quota importante di budget per l'acquisto e il rinnovo dell'hardware.

Un pool comune

L'astrazione dei Virtual Research Environment permette di allocare quote di risorse corrispondenti all'hardware acquistato in un progetto mantenendo una sola infrastruttura fisica.

1

Avvio

Hardware PNRR installato

2 uplink da 100 Gb/s per leaf (circa 6:1)

2

Crescita

Nuovi server e apparati fino a riempire i rack già installati

Uplink a 4, poi 6 per leaf (circa 2:1)

3

Rinnovo

Sostituzione dei server obsoleti con fondi di progetto

Hardware dismesso riusato per laboratorio e bare metal

16 leaf
con 4 uplink, sulle 64 porte degli spine

4 spine
estensione possibile del fabric

EC 4+2
praticabile con più coppie di leaf



(2 min) D4Science partecipa da parecchi anni a progetti europei e prevede una quota importante di budget per l'acquisto e il rinnovo dell'hardware. Questo ci ha permesso di pianificare fin dall'inizio due cose: la sostituzione dell'hardware quando diventerà obsoleto, e l'aumento di server e apparati di rete fino a riempire i rack già installati. Il fabric è dimensionato per crescere: gli spine hanno 64 porte a 100 Gb/s, sufficienti per sedici leaf con quattro uplink ciascuno, e si può passare a quattro spine. Gli uplink per leaf partono da due e salgono a quattro, poi a sei. Con più coppie di leaf diventa praticabile anche l'erasure coding per lo storage. Con l'astrazione dei Virtual Research Environment possiamo assegnare a ogni progetto quote di risorse corrispondenti all'hardware che ha acquistato, mantenendo una sola infrastruttura fisica; questo semplifica la governance fra i partner.

Grazie

Franca Debole, responsabile del gruppo S2I2S
Tommaso Piccioli e Marco Procaccini, S2I2S
Gruppo reti, CNR-IIT
Guest star: Ermann Ripepi, CNR-IMAA

S2I2S: Servizio Infrastruttura Informatica e Supporto ai Servizi, CNR-ISTI

andrea.dellamico@isti.cnr.it · www.d4science.org

WORKSHOP GARR 2026
NET MAKERS

Grazie

Franca Debole, responsabile del gruppo S2I2S
Tommaso Piccioli e Marco Procaccini, S2I2S
Gruppo reti, CNR-IIT
Guest star: Ermann Ripepi, CNR-IMAA
S2I2S: Servizio Infrastruttura Informatica e Supporto ai Servizi, CNR-ISTI

Ringrazio chi lavora con me a questa attività: Franca Debole, responsabile del gruppo S2I2S, Tommaso Piccioli e Marco Procaccini, il gruppo reti del CNR-IIT ed Ermann Ripepi del CNR-IMAA.

Domande

Per le domande

www.partici.fi

codice **83995288**

WORKSHOP GARR 2026

NET MAKERS

2026-11-02

Domande

Per le domande
www.partici.fi
codice **83995288**

Per le domande, dalla sala o da remoto: Particify, con il QR code oppure su www.partici.fi con il codice 83995288.