WORKSHOP GARR 2025

NET MAKERS

DNS-HA @INFN: garantire continuità operativa e affidabilità nei servizi di naming

Lorenzo Chiarelli

GARR

Introduzione

- Alcuni servizi **non** dispongono nativamente di un sistema di **HA geografica** ma lo implementano a livello di **DNS** (siti web, SMTP ecc.)
- Serve un meccanismo di reindirizzamento automatico/manuale in caso di manutenzione, guasto o disastro.

Obiettivo:

- Garantire **continuità di servizio**
- Aumentare la **resilienza**
- Consentire **gestione distribuita** del naming
- Ridurre al **minimo l'impatto** sugli utenti

Da master slave a multimaster

DNS master slave «classico»

```
servizio.infn.it 60 IN A 131.154.52.10
                 60 IN A 192.84.150.20
```

`infn.it` non permette modifiche

(scelta implementativa)

dinamiche/automatiche

Modifica manuale **del** master

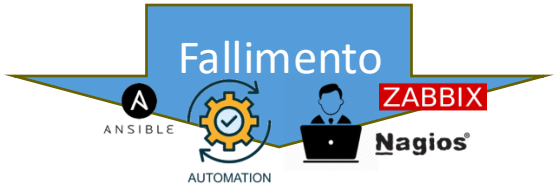
```
servizio.infn.it ~~60 IN A 131.154.52.10~~
                 60 IN A 192.84.150.20
```

E se il master è down o gli amministratori non sono raggiungibili?

DNS-HA multimaster

```
servizio.infn.it  IN CNAME servizio.ha.infn.it
servizio.ha.infn.it  60 IN A 131.154.52.10
                     60 IN A 192.84.150.20
```

`ha.infn.it` permette di operare dinamicamente/automaticamente



Modifica automatica/manual **dei** master

```
servizio.ha.infn.it  ~~60 IN A 131.154.52.10~~
                     60 IN A 192.84.150.20
```

fornisce un quarto livello ai gruppi di Lavoro

`gruppo.ha.infn.it`

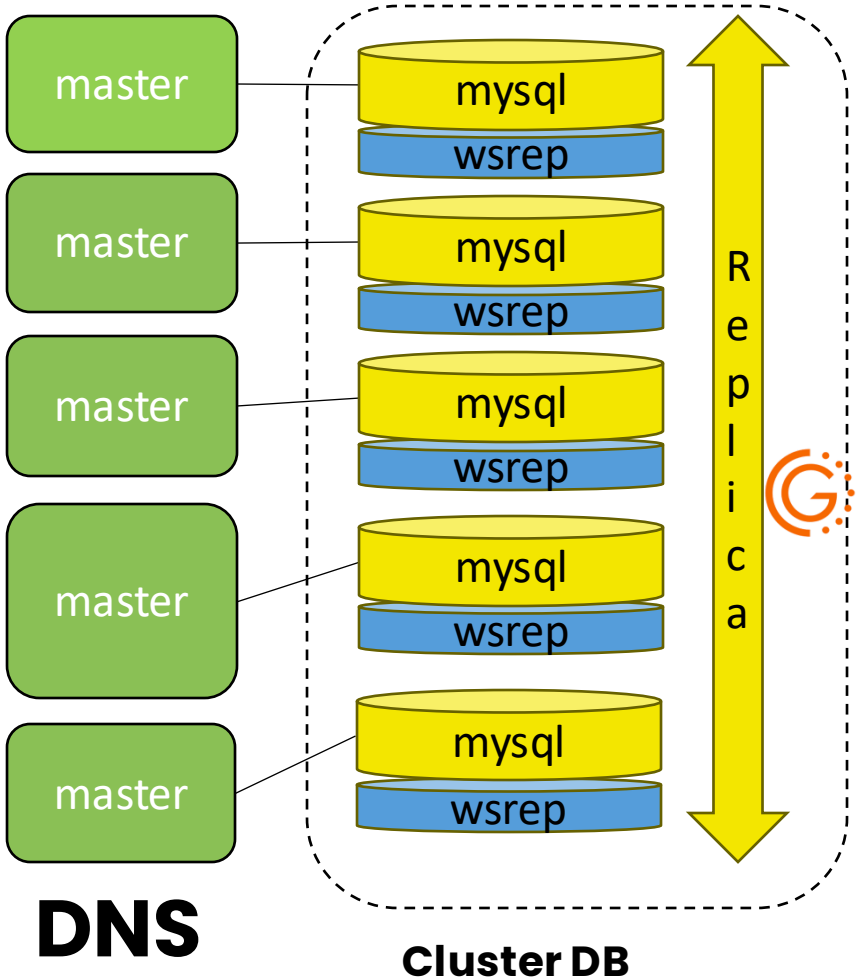
che possono operare in autonomia

Suddivisione del dominio amministrativo

Architettura multi master in HA geografica requisiti

- Nodi **distribuiti geograficamente**
- Ogni nodo deve essere **autoritativo e paritetico**
- Possibilità di **operare su qualsiasi master**
- **Scincronizzazione automatica** dei record DNS tra i nodi
- In caso di nodo non raggiungibile:
  - Il servizio DNS **rimane operativo**
  - Le modifiche vengono sincronizzate **al suo ritorno**

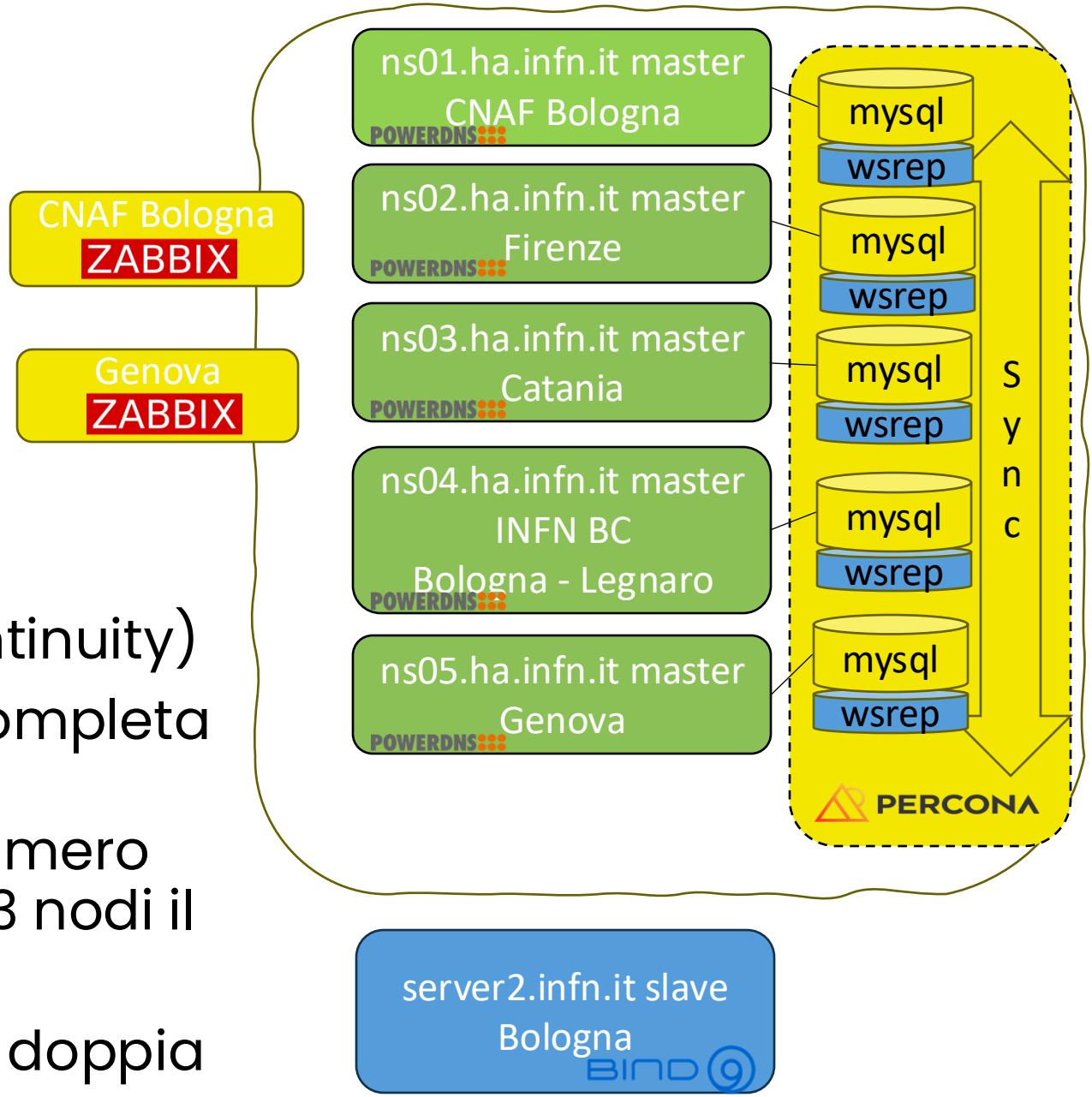
- WriteSetReplication (wsrep)
  definisce un insieme di API per la replicazione dei dati di un'applicazione.



Galera implementa wsrep multi-master per mysql

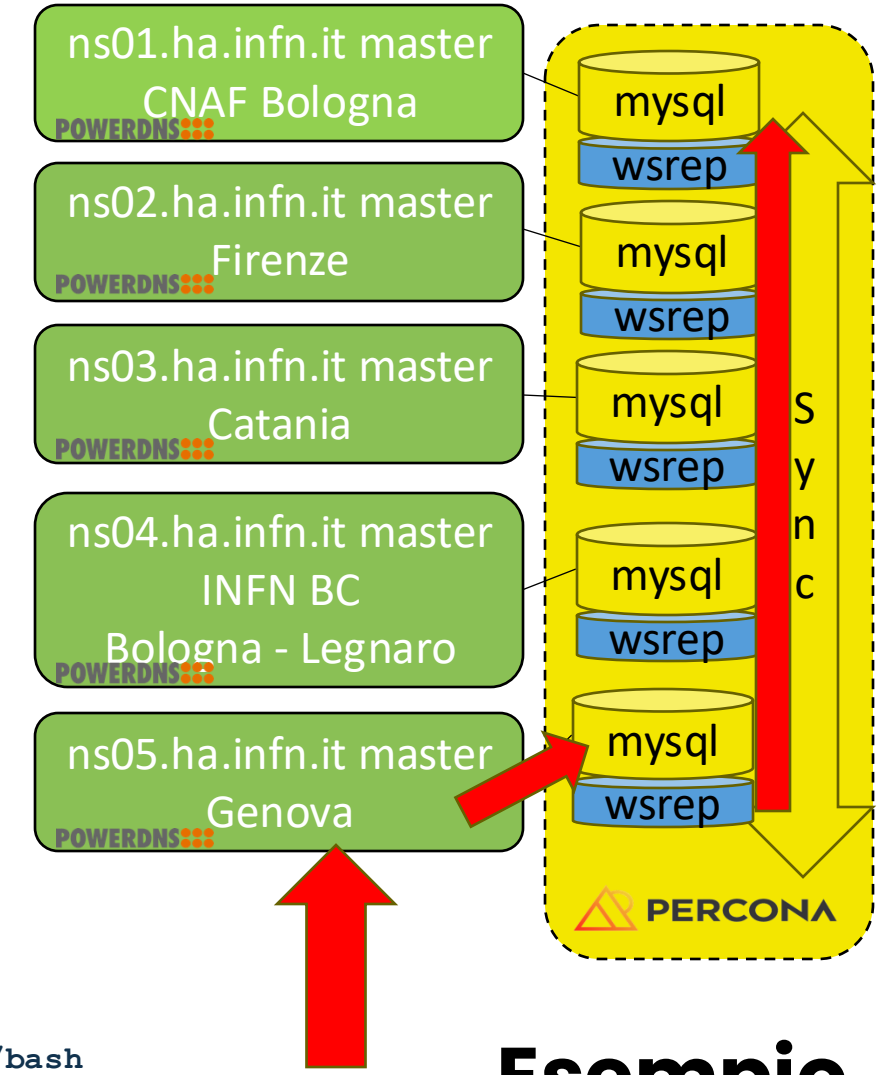
Implementazione

- **OS:** Rocky Linux 9
- **DNS**: POWERDNS (backend mysql)
  - CLI `pdnsutil`
  - Interfaccia web PowerAdmin
- Database: PERCONA xtradb cluster
  - Galera+mariadb
- 5 master su 4 sedi (+1 Business Continuity)
- 1 slave (bind 9) in caso di Perdita completa del cluster percona
  - Il cluster è garantito con un numero minimo di 3 nodi con meno di 3 nodi il cluster diventa in sola lettura
- Monitoraggio e allarmistica: Zabbix doppia istanza CNAF e GENOVA



Interazione con il servizio

- Ad ogni zona viene associate una chiave tsig
  - `aai-ha-key. hmac-sha256. [KEY]`
  - `nsupdate` con chiave tsig
- Le modifiche sono abilitate da alcuni nodi autorizzati + bastione di emergenza
  - ACL sul file pdns.conf -> `allow-dnsupdate-from`
- Ogni gruppo **gestisce autonomamente** la propria zona la aggiorna con I meccanismi automatici/manuali che preferisce.



- Attualmente viene usato dal gruppo mailing **`mailing.ha.infn.it`** per ridondare geograficamente gli SMTP utilizzati da INFN Cloud e alcuni Servizi nazionali

Esempio

```
#!/bin/bash
  nsupdate <<!
  server ns05.ha.infn.it 53
  zone aai.ha.infn.it
  update add test.aai.ha.infn.it 60 A 131.154.52.206
  key hmac-sha256:aai-ha-key [KEY]
  send
  !
```

Garantire l’operatività

- Gruppo di amministratori composto da almeno una persona per sito (dnsha-support@lists.infn.it)
- Allineamenti mensili, documentazione condivisa

- Ogni sito gestisce in autonomia la propria macchina con i propri tool locali (provisioning,monitoring,allarmistica,backup ecc.)

- Tutti gli amministratori possono operare su qualsiasi altro nodo garantendo l’operatività su tutti i siti

Sviluppi futuri

- Rendere disponibili agli utenti le API di Powerdns
- Armonizzare la distribuzione della configurazione
  - playbook ansible condivisi (es. distribuzione di pdns.conf per le ACL)
- Verrà adottato dal gruppo Disaster Recovery
- Sistema disponibile per il Sistema Informativo e AAI dell'ente
- logging e backup centralizzati

Grazie

Contatti:

dnsha-support@lists.infn.it

Bologna: Lorenzo Chiarelli Stefano Antonelli

Genova: Mirko Corosu

Firenze: Leandro Lanzi

Catania: Salvatore Monforte

WORKSHOP GARR 2025

NET MAKERS