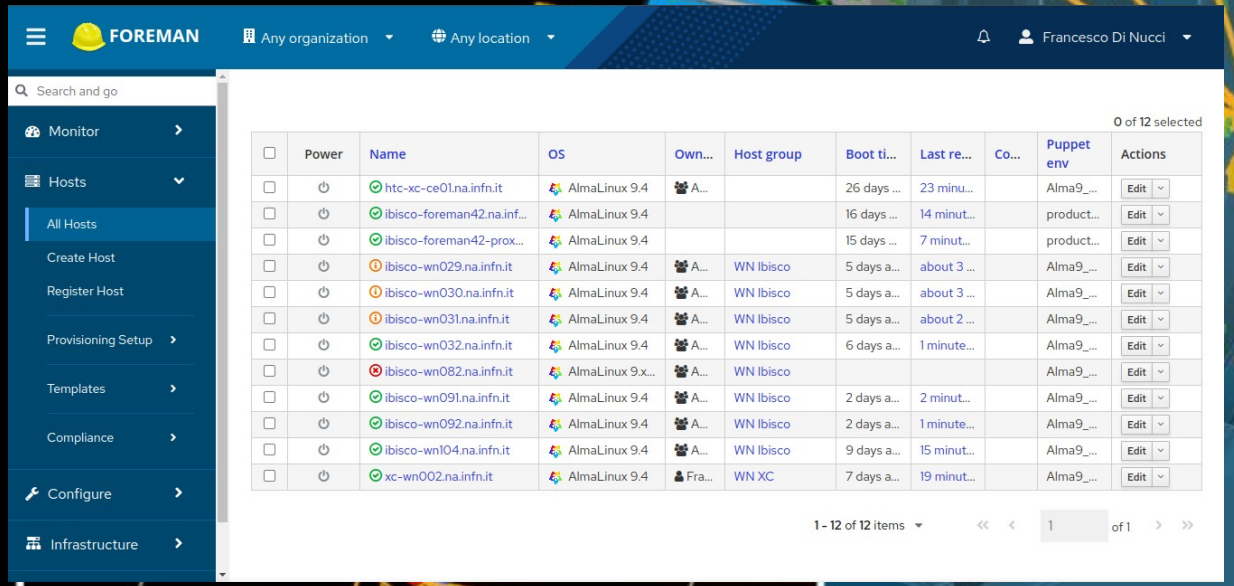
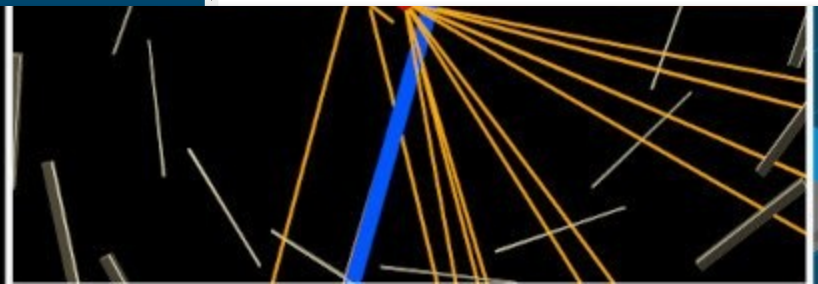
Foreman per deploy WN ATLAS su AlmaLinux 9

Alessandra Doria, Bernardino Spisso, Francesco Di Nucci



Dalla macchina vuota ad un WN pronto in pochi minuti:

- Sistema Operativo
- Installazione Pacchetti
- Configurazione
- Completamente Unattended
- Idempotente
- Scalabile



ATLAS EXPERIMENT

INFN

Funzionalità

Foreman 3.12.x

- DHCP
- PXE/TFTP
- Installazione SO via kickstart
- Visualizzazione report periodici

Puppet 8.x + r10k

- Installazione pacchetti
- Configurazione
- Cifratura secrets con hiera-eyaml
- Environment via Baltig (git/GitLab INFN)

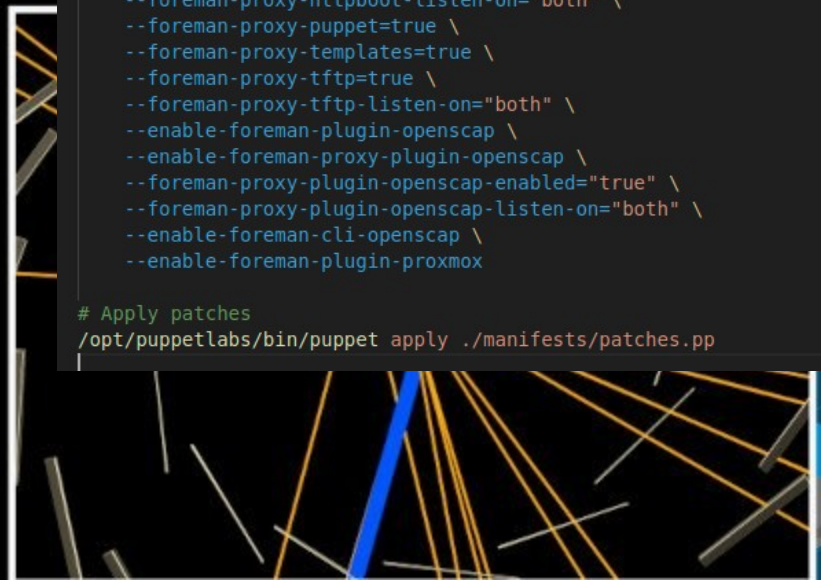
ATLAS EXPERIMENT

INFN

Foreman - Installazione

```
foreman-installer --foreman-email-delivery-method="smtp" \
    --foreman-email-smtp-address="smtp.na.infn.it" \
    --foreman-email-smtp-port=25 \
    --foreman-initial-admin-email="ibisco-ops@lists.na.infn.it" \
    --foreman-proxy-dhcp=true \
    --foreman-proxy-dhcp-interface="ens18" \
    --foreman-proxy-dhcp-listen-on="both" \
    --foreman-proxy-dhcp-managed=true \
    --foreman-proxy-dhcp-nameservers="192.84.134.50,192.84.134.55" \
    --foreman-proxy-dhcp-netmask="255.255.0.0" \
    --foreman-proxy-http=true \
    --foreman-proxy-httpboot=true \
    --foreman-proxy-httpboot-listen-on="both" \
    --foreman-proxy-puppet=true \
    --foreman-proxy-templates=true \
    --foreman-proxy-tftp=true \
    --foreman-proxy-tftp-listen-on="both" \
    --enable-foreman-plugin-openscap \
    --enable-foreman-proxy-plugin-openscap \
    --foreman-proxy-plugin-openscap-enabled="true" \
    --foreman-proxy-plugin-openscap-listen-on="both" \
    --enable-foreman-cli-openscap \
    --enable-foreman-plugin-proxmox

# Apply patches
/opt/puppetlabs/bin/puppet apply ./manifests/patches.pp
```

- Script bash per foreman-installer (metodo raccomandato di installazione)
- Passaggi manuali di fine installazione automatizzati con manifest Puppet
- Upgrade major gestito tramite task Bolt (strumento Puppet per pianificazione task)
- Tutto realizzato appositamente e disponibile su Baltig, da adattare in base alle esigenze di sezione

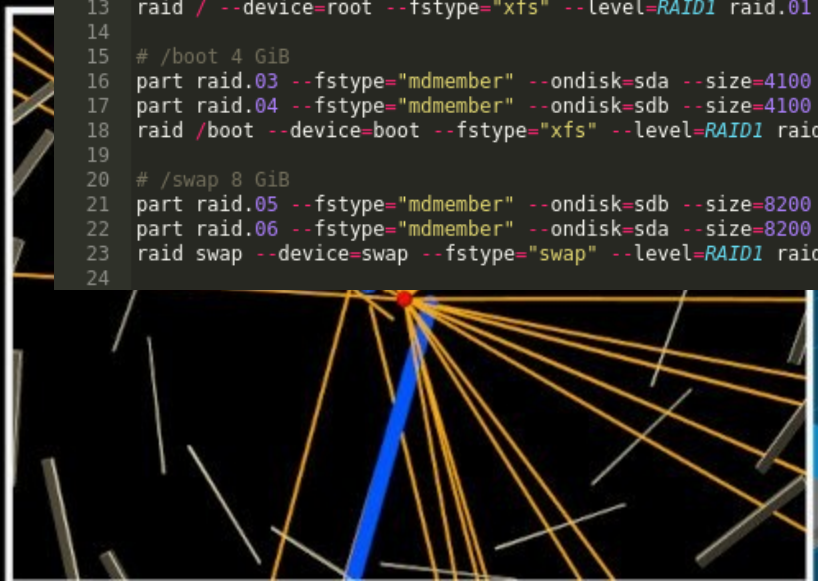


ATLAS EXPERIMENT

INFN

WN - EL9 con kickstart

```
# Use only two disks
ignoredisk --only-use=sda,sdb
# Partition clearing information
clearpart --all --initlabel

# biosboot partition
part biosboot --fstype="biosboot" --ondisk=sda --size=1
part biosboot --fstype="biosboot" --ondisk=sdb --size=1

# /
part raid.01 --fstype="mdmember" --ondisk=sda --size=3650528
part raid.02 --fstype="mdmember" --ondisk=sdb --size=3650528
raid / --device=root --fstype="xfs" --level=RAID1 raid.01 raid.02

# /boot 4 GiB
part raid.03 --fstype="mdmember" --ondisk=sda --size=4100
part raid.04 --fstype="mdmember" --ondisk=sdb --size=4100
raid /boot --device=boot --fstype="xfs" --level=RAID1 raid.03 raid.04

# /swap 8 GiB
part raid.05 --fstype="mdmember" --ondisk=sdb --size=8200
part raid.06 --fstype="mdmember" --ondisk=sda --size=8200
raid swap --device=swap --fstype="swap" --level=RAID1 raid.05 raid.06

```



Kickstart

- Metodo standard per installazione unattended di Enterprise Linux (RHEL e derivate, Fedora, CentOS Stream…)
- Non è statico, viene generato da Foreman con template Ruby controllati da variabili
- Template custom per i WN con UID/GUID dell'utente condor parametrizzato
- Tabella partizioni personalizzabile

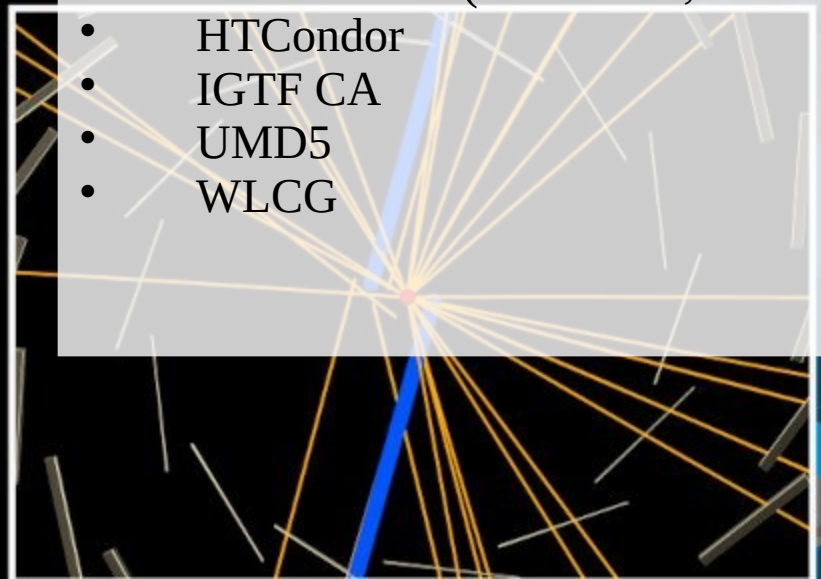
ATLAS EXPERIMENT

INFN

WN - Ambiente Puppet

Repository

- CernVM
- Elasticsearch (facoltativo, monitoring)
- HTCondor
- IGTF CA
- UMD5
- WLCG



Pacchetti

- Auditbeat (facoltativo, monitoring)
- CA EGI
- CVMFS
- Ganglia
- Htcondor
- VOMSes
- Wn metapackage
- Zabbix (facoltativo, monitoring)

WN – Configurazione rete

- Tutti i WN sono su rete privata divisa in VLAN, con rotte statiche
- Dopo la fase di installazione via PXE, la configurazione di rete viene resa statica, in caso di downtime del DHCP
- L’ambiente Puppet ha MAC e IP di ogni WN in Hiera
- Un manifest Puppet ricava il nome dell’interfaccia a partire dal MAC in Hiera e crea il file `/etc/NetworkManager/system-connections/${interface_name}.nmconnection` con la configurazione desiderata (IP, subnet, gateway, rotte statiche...)

Puppet - hiera-eyaml

```
# | This is eyaml edit mode. This text (lines starting with # | at the top of
# | the file) will be removed when you save and exit.
# |  - To edit encrypted values, change the content of the DEC(<num>)::PKCS7[]!
# |    block.
# |    WARNING: DO NOT change the number in the parentheses.
# |  - To add a new encrypted value copy and paste a new block from the
# |    appropriate example below. Note that:
# |     * the text to encrypt goes in the square brackets
# |     * ensure you include the exclamation mark when you copy and paste
# |     * you must not include a number when adding a new block
# |    e.g. DEC::PKCS7[]!
---
test::key: >
  DEC::PKCS7[Informazione segretissima]!
~
```

```
$ cat test.eyaml
---
test::key: >
  ENC[PKCS7,MIIBiQYJKoZIhvcNAQcDoIIBejCCAXYCAQAxggEhMIIBHQIBAD
  AFMAACAQEwDQYJKoZIhvcNAQEBBQAEggEAcOJvntICCsi2oZN2bZA2IWI+nK
  d8zNOL26hS9qENvOhQg12sNW0fGbgBt6jKvmPM21lezsFqTHc86RISW0t0aa
  Sl8NJymzbIMJA6e6FytxYrAbipkgLrJUZO/NebXoCmGxuv6PaHKGfbDNscY7
  DmsGqKWX0cp5WAWmuveqaJNnQXICZuixLsD5XL4dWL1EmpkqlSnM+jRmDdQk
  LTgZonRLFGmZz1BG8HHoTcXTb1Khbg3XZ+W6y8gXRsHZU6y5rVQIkbgwSagJ
  JV045IBtlagu6Kb1lhC1m1i+laF82mfrcyKkhQWX85dX/y7/9CRBcx/3CSyx
  h79tgWoEbfjFcz5jBMBgkqhkiG9w0BBwEwHQYJYIZIAWUDBAEqBBCxiLWXnx
  ysniDyLbaoku2tgCDMTjctmOkj0FubvSsz4LWyVLOOa+SHSMwr7BpGp+QJHA
  ==]
```

- Hiera-eyaml è un backend per Hiera che permette di criptare determinati valori tramite coppia chiavi pubblica/privata
- Ambienti con valori criptati possono essere anche ospitati su repository GIT condivise
- Solamente i sysadmin e il server Foreman/Puppet hanno copia delle chiavi
- Può essere utilizzato separatamente da Foreman

ATLAS EXPERIMENT

INFN

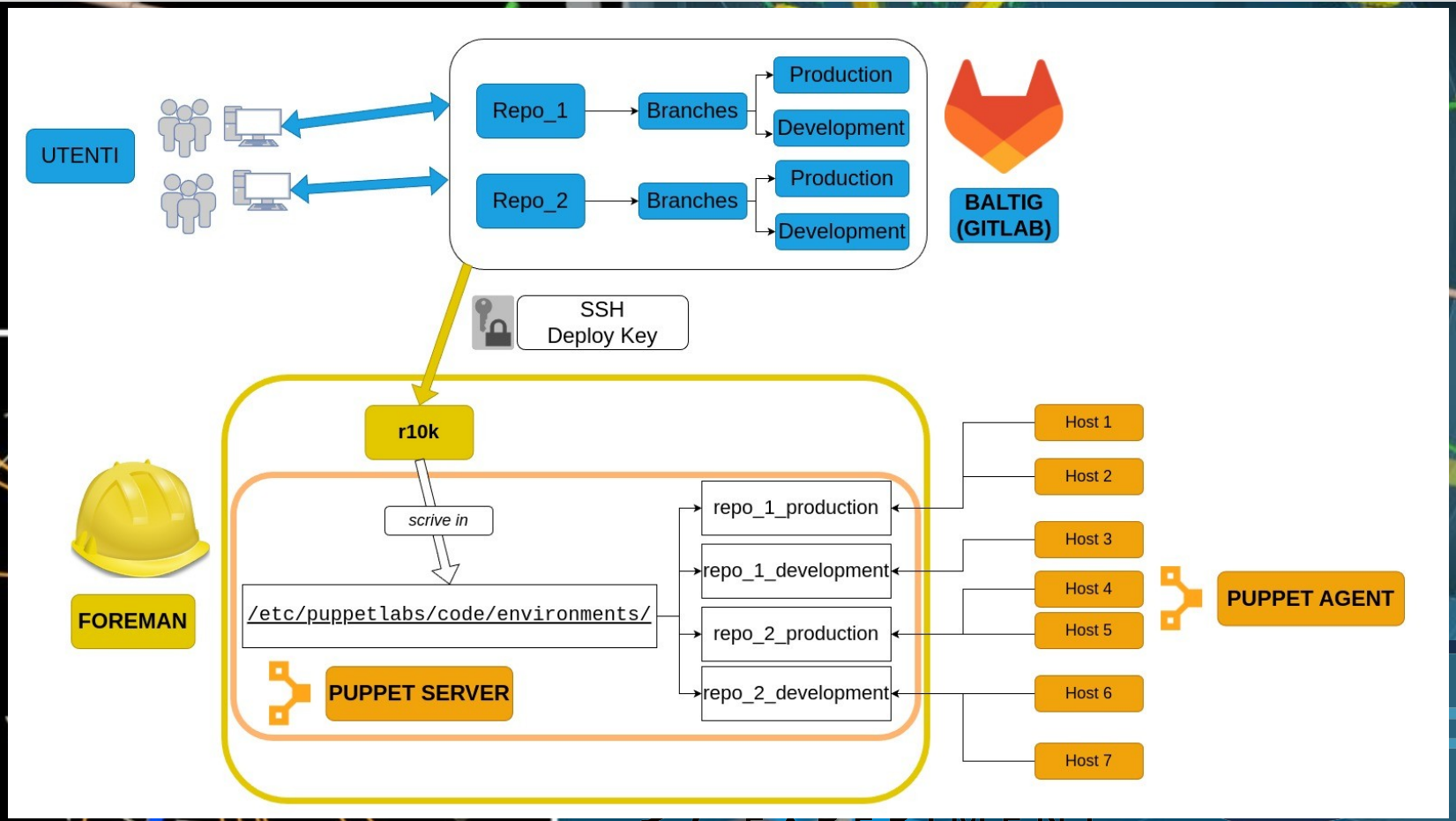
Workflow iniziale

- Installazione Foreman ed eventuali Smart Proxy
- Setup dominio e reti/sottoreti
- Creazione sistemi operativi ed associazione Installation Media
- Eventuale modifica template ed associazione ad OS
- Importazione ambienti Puppet
- Creazione host
- Boot degli host via PXE

Workflow Puppet + r10k

- Gli ambienti Puppet si trovano in repository GIT condivise su Baltig/GitHub/etc. (preferibilmente con secret criptati tramite hiera-eyaml)
- Le modifiche si effettuano sulla propria macchina ed inviano alla repository con git add/commit/push/etc
- Accesso SSH a Foreman, esecuzione “r10k deploy”
- Gli ambienti verranno aggiornati sulla base della repository git
- Gli agent provvederanno ad allineare le macchine all’environment aggiornato

Puppet - r10k


UTENTI
Repo_1
Branches
Production
Development
Repo_2
Branches
Production
Development
BALTIG (GITLAB)
SSH Deploy Key
r10k
scrive in
/etc/puppetlabs/code/environments/
repo_1_production
repo_1_development
repo_2_production
repo_2_development
PUPPET SERVER
FOREMAN
Host 1
Host 2
Host 3
Host 4
Host 5
Host 6
Host 7
PUPPET AGENT

Sviluppi Futuri

- Passaggio a boot UEFI + HTTPBOOT
- Runner + CI/CD Baltig per linting/test
- Passaggio UI web a certificati non autofirmati
- Valutazione plugin (Ansible, BMC, OpenSCAP...)
- Aggiornamenti security automatici via dnf-automatic con esecuzione automatica foreman-installer per evitare cambiamenti indesiderati

Sviluppi futuri Puppet WN

- Come collaborare?
- Modulo parametrizzato condiviso e repository con ambiente private?
- Per iniziare, repository read-only?

Approfondimenti

- Foreman
  - Foreman-installer
  - IbiscoCloud Foreman Installer (richiede accesso a Baltig)
  - Setup r10k/g10k and Foreman – Foreman Community
- Hiera-eyaml
  - Hiera-Eyaml: How to Use It - Puppet Blog
  - HOWTO Set Up and Utilize hiera-eyaml - SIMP docs
- Kickstart
  - Kickstart Documentation – Pykickstart
  - Kickstart commands and options reference – RHEL9 documentation
- r10k
  - Fattening the workflow, part 2: r10k – Puppeteers blog
  - puppet-r10k
  - R10k – Puppet Enterprise docs (si applica anche a Puppet Open Source)