Red Hat Consulting

Crédit Agricole

OpenShift Container Platform 4.14

Documento di installazione

Ambiente di Parallelo

Confidentiality, Copyright, and Disclaimer

This is a Customer-facing document between Red Hat, Inc. and Crédit Agricole.

This document is not a quote and does not include any binding commitments by Red Hat.

Trademarks

Trademarked names may appear throughout this document. Rather than list the names and entities that own the trademarks or insert a trademark symbol with each mention of the trademarked name, the names are used only for editorial purposes and to the benefit of the trademark owner with no intention of infringing upon that trademark.

Review History

Version	Date	Contributor	Role	Description
1.0	08/04/2024	Giulia Bacchini	Senior Cloud Consultant	Installazione HUB e Acilia
1.0	16/04/2024	Matteo Santucci	Senior Cloud Consultant	Installazione Quay

Table of Contents

1. Introduzione **5**
1.1. Purpose 5
1.2. Termini e acronimi 5
2. Cluster HUB di management **7**
2.1. Installazione cluster base 7
2.2. Installazione ACM 11
2.3. Configurazioni aggiuntive 12
2.3.1. Servizio Chronyd 13
2.3.2. Definizione nodi infrastrutturali 16
2.3.3. Autenticazione tramite LDAP 19
2.3.4. Sync gruppi di utenti tra alberatura LDAP e OCP 22
3. Cluster di Acilia **27**
3.1. Installazione cluster base 27
3.2. Configurazioni aggiuntive 37
3.2.1. Nodi worker 37
3.2.2. Servizio Chronyd 39
3.2.3. Definizione nodi infrastrutturali 41
3.2.4. Definizione nodi storage 43
3.2.4.1. Aggiunta dischi per ODF 45
3.2.5. Installazione ODF 45
3.2.5.1. Local storage operator 46
3.2.5.2. Openshift Storage operator 48
3.2.6. Moving ingress su nodi infrastrutturali 51
3.2.7. Moving monitoring su nodi infrastrutturali 53
3.2.8. Autenticazione tramite LDAP 55
3.2.9. Sync gruppi di utenti tra alberatura LDAP e OCP 59
3.2.10. Installazione componente di logging 64
3.2.11. Installazione Quay 69
3.2.11.1. Quay Operator 69
3.2.11.2. Schedulazione all’interno dei nodi infra 73
3.2.11.3. Storage PostgreSQL 73
3.2.11.4. Autenticazione LDAP 74

1. Introduzione

Red Hat è stata ingaggiata da Crédit Agricole per installare l'ambiente di Parallelo.

Tale ambiente è costituito dai seguenti cluster:

- Un cluster di management che ospita la componente ACM, installato nel DC del sito di Acilia e identificato con il nome **ocp-parallelo** o **acm-hub**.
- Un cluster OCP di Parallelo installato sul DC del sito di Acilia e identificato con il nome **ocp1-parallelo**
- Un cluster OCP di Parallelo installato sul DC del sito di Rozzano e identificato con il nome **ocp2-parallelo**

Questo documento tratta l'installazione dei tre cluster e le configurazioni dei vari servizi a contorno.

La modalità di installazione scelta per questi ambienti è la "IPI", la versione di OpenShift Container Platform scelta è la **4.14.2**, per uniformità con l'ambiente di Collaudo, la piattaforma sottostante è il vSphere.

1.1. Purpose

Questo documento descrive la procedura di installazione dei cluster e le configurazioni apportate ai vari servizi compresi.

1.2. Termini e acronimi

La tabella di seguito indica il significato di alcuni termini e acronimi utilizzati nel documento.

Acronym	Description
RH	Red Hat, Inc
RHEL	Red Hat Enterprise Linux
AD	Active Directory
CA	Certificate Authority
DC	Data Centre
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol

FQDN	Fully Qualified Domain Name
Guest	Also see “VM”. This is virtual machine running on a Host.
HA	High-Availability or Highly-Available
Host	The physical hardware or the logical OS which runs virtualisation technology allowing one or more Guest OS’s to run on the hardware owned by the Host
Compute Nodes	Compute nodes dedicated to host end user containers and apps
Infrastructure Nodes	Compute nodes reserved to host infrastructure services like routing layer/metrics/logging
Master Node	Node acting as controller for OCP, exposing api and hosting cluster configuration
IPI	Installer Provided Infrastructure
OS	Operating System
OCP	OpenShift Container Platform
SAN	Storage Area Network
SSL	Secure Sockets Layer
VIP	Virtual IP address
VLAN	Virtual LAN is a networking virtualisation technology
VXLAN	Virtual Extensible LAN (VXLAN) is a network virtualisation technology
Workload	Synonym for “Guest” or “VM”
OCP	Openshift Container Platform
ODF	Openshift Data Foundation
RHACM	Red Hat Advanced Cluster Management
AZ	Availability Zone
HA	High Availability

2. Cluster HUB di management

2.1. Installazione cluster base

La piattaforma che ospita il cluster OCP di management è un vSphere in versione 7.0.3 , compatibile con la versione di OCP scelta, la 4.14.2.

Tale cluster è composto dalle seguenti macchine virtuali:

Ruolo	vCPU	RAM	OS disk	Count
Master	16	32	120 GB	3
Infra	16	32	120 GB	3

Come attività preliminari all'installazione sono stati eseguiti i seguenti task:

- Impostazione del proxy sul bastion **grpi-ocp-hv00**
- Creazione della directory di lavoro **/root/ocp-acm/installation_dir**
- Creazione chiave ssh per l'accesso ai nodi OCP **/root/.ssh/ocp-parallelo**
- Download client e installer in versione **4.14.2**
- Copia in locale dei certificati del vCenter

Seguono i comandi utilizzati:

```
Python
--- Creazione directory di lavoro ---

[root@grpi-ocp-hv00 ~]# mkdir ocp-acm
[root@grpi-ocp-hv00 ~]# cd ocp-acm
[root@grpi-ocp-hv00 ocp-acm]# mkdir installation_dir

--- Impostazione proxy ---

[root@grpi-ocp-hv00 ocp-acm]# export https_proxy=http://vip-navproxy-server.cariprpc.it:8080
[root@grpi-ocp-hv00 ocp-acm]# export http_proxy=http://vip-navproxy-server.cariprpc.it:8080
[root@grpi-ocp-hv00 ocp-acm]# export no_proxy=localhost,127.0.0.1,localaddress,.localdomain.com,.cariprpc.it,10.68.0.0/14,172.27.0.0/16,10.215.87.0/24
```

```
--- Download client e installer ---

[root@grpi-ocp-hv00 ocp-acm]# wget
https://mirror.openshift.com/pub/openshift-v4/x86_64/clients/ocp/4.14.2/openshift-i
nstall-linux.tar.gz
[root@grpi-ocp-hv00 ocp-acm]# wget
https://mirror.openshift.com/pub/openshift-v4/x86_64/clients/ocp/4.14.2/openshift-c
lient-linux-4.14.2.tar.gz
[root@grpi-ocp-hv00 ocp-acm]# ls -ltr
total 483140
-rw-r--r-- 1 root root  63934993 Nov 10 08:33 openshift-client-linux-4.14.2.tar.gz
-rw-r--r-- 1 root root 430795428 Nov 10 08:33 openshift-install-linux.tar.gz
[root@grpi-ocp-hv00 ocp-acm]# tar zxvf openshift-install-linux.tar.gz -C /usr/bin
README.md
openshift-install
[root@grpi-ocp-hv00 ocp-acm]# chmod +x /usr/bin/openshift-install
[root@grpi-ocp-hv00 ocp-acm]# tar zxvf openshift-client-linux-4.14.2.tar.gz -C
/usr/bin
README.md
oc
kubectl
[root@grpi-ocp-hv00 ocp-acm]# chmod +x /usr/bin/oc
[root@grpi-ocp-hv00 ocp-acm]# oc completion bash > /etc/bash_completion.d/openshift

--- Installazione certificati vCenter ---

[root@grpi-ocp-hv00 ~]# cd  /home/GBCAI/j51890-cyberark/
[root@grpi-ocp-hv00 j51890-cyberark]# cp certs/lin/*
/etc/pki/ca-trust/source/anchors
[root@grpi-ocp-hv00 j51890-cyberark]# update-ca-trust

--- Generazione chiave ssh ---

[root@grpi-ocp-hv00 ocp-acm]# ssh-keygen -t ed25519 -N '' -f ~/.ssh/ocp-parallelo
Generating public/private ed25519 key pair.
Your identification has been saved in /root/.ssh/ocp-parallelo
Your public key has been saved in /root/.ssh/ocp-parallelo.pub
The key fingerprint is:
SHA256:LgYRq643Ll3Hzeti/Z7EkdxVEgq2NBX//1kSuvh+aSc root@grpi-ocp-hv00
The key's randomart image is:
+--[ED25519 256]--+
|      .    =.o.o..|
|      o   o + o o |
|      o     . . o |
|   . .   . o . . |
|  . .. oS + . . .|
| .  ..o.o. . . ..|
| ... .o...o . ..o|
|..+  .o.o. o .E.=|
|.+.. . o.o=o+o +.|
+----[SHA256]-----+
[root@grpi-ocp-hv00 ocp-acm]# eval "$(ssh-agent -s)"
Agent pid 54467
[root@grpi-ocp-hv00 ocp-acm]# ssh-add /root/.ssh/ocp-parallelo
Identity added: /root/.ssh/ocp-parallelo (root@grpi-ocp-hv00)
```

A questo punto è stato preparato l'*install-config.yaml* che riportiamo:

Python

```
apiVersion: v1
baseDomain: cariprpcpar.it
proxy:
  httpProxy: http://vip-navproxy-server.cariprpc.it:8080
  httpsProxy: http://vip-navproxy-server.cariprpc.it:8080
  noProxy:
localhost,127.0.0.1,localaddress,.localdomain.com,.cariprpcpar.it,172.30.0.0/16,.ca
riprpc.it,10.215.87.0/24
compute:
- name: worker
  hyperthreading: Enabled
  platform:
    vsphere:
      cpus: 16
      coresPerSocket: 2
      memoryMB: 32768
      osDisk:
        diskSizeGB: 120
  replicas: 3
controlPlane:
  hyperthreading: Enabled
  name: master
  platform:
    vsphere:
      cpus: 16
      coresPerSocket: 2
      memoryMB: 32768
      osDisk:
        diskSizeGB: 120
  replicas: 3
metadata:
  name: ocp-parallelo
networking:
  machineNetwork:
  - cidr:  10.215.87.0/24
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  vsphere:
    apiVIP: 10.215.87.4
    cluster: "OCP_PREPROD"
    datacenter: "ACILIA"
    defaultDatastore: ESX-OCP-PREPROD-AC-0000
    ingressVIP: 10.215.87.3
    network: "dvpg_620_DMZ_ocprhel_par"
    password: 'XXXXXXXXXXXXXX'
    username: cariprpc\cp_12_vcenter_OCP
    vCenter: ac-cags-vcsa001.cariprpc.it
    folder: "/ACILIA/vm/PARALLELO/OCP"
publish: External
```

```
pullSecret:
'{"auths":{"cloud.openshift.com":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc
3NfZTdjYzcwZDhkNjZlNGE1MTgxYWZlOTAzYTNiMTI2NDk6TjZHSFpKUTI4RFExNEgzT05PVlQ2UTZYUU4z
MU40UU9TVzRYTFNEVjdUOElBVDA3V01VTFpVSFBFQzRYTkFSVg==","email":"daniele.bagiotti@cre
dit-agricole.it"},"quay.io":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc3NfZT
djYzcwZDhkNjZlNGE1MTgxYWZlOTAzYTNiMTI2NDk6TjZHSFpKUTI4RFExNEgzT05PVlQ2UTZYUU4zMU40U
U9TVzRYTFNEVjdUOElBVDA3V01VTFpVSFBFQzRYTkFSVg==","email":"daniele.bagiotti@credit-a
gricole.it"},"registry.connect.redhat.com":{"auth":"fHVoYy1wb29sLTgxNGFiODI0LTgwMzc
tNGJjMy1iMTA2LWUwZDQyMWY5NDU2ZjpleUpoYkdjaU9pSlNVelV4TWlKOS5leUp6ZFdJaU9pSTJNekZpWW
1Ka09XTXlOVGswWTJaak9UWm1abUkwWVRRMU4yTmhORE00TVNKOS5jdVU0TjA4R3Q5VUh6Snk0d3VXOV9ae
FdTc1FiN0dUYThWRm0yTTdqWFBmSXd3TXZ0YnZGTHVwYno5bTZZX3VXTE91UF9SZk9xSVpldGk1X3oxUnBN
OFVnRDMzUUJ2V2QxbGFxMkJEY0ZUTHlyQ2Z5anVvaGdvZFppZE5SRFgwQXRURFdDLTlOMmRlMTZMUWhaeUt
tYnBaZlFDVVo5TGtDLWdQSk1xVmNTOFY3RzhXM2x0QWkyTm55TGp1dzBDMk5MUjl3M3R4M29tRnhES1Jabm
1kYmFQemdzQ2o4bnNCZXhDYmtYRFVCVWo1YUFjX1Fha3FxNVZZYmtxYTQtNHRZYTljamc3RXEtUy11dW5pW
lo3cldxLUhOdmlYRUpWVVY0M1NkdnlNZ2I0bTQwanFaYVpqOVpLQ1pycktKVUdnd0tTS1IteUNwcHhWZWZS
cnB0QmZ4WndrM0ZPNGg1azZuOUdOSE1RazdmRGVnTEJ5WVdmcVdQNnZHSENudW1LRVFBLWczcXBPZENrWlp
tV2VRQlpHaExHNkhpS0luRHVIOUxKb2hhSm5BcTBqVVhsVHdGYWZ4OUtoVXhUemM1cDhBUmQwZGdEd2tUZj
JaVWZKM2czVW1QUjNHaTRmY2xTaHc5RW9UbXlKXzYzdHpSV0pJd053X0VSOE9QSHVnNFNwM2pfZ2lPaXNCS
mI2TU5ybkJ3WmFXWElDNjdCbnR2REJVTXgyZkdYbDJ2cDZEamdpWjZxU2Z5blRwWXFpaFBGSWplbldQd0Vq
UFl5b01nQTF2NVJoanppT1ZCemZXRTVKY1pOdC1VaU5GckdaMmV0bXdQUkpNaThJODJ2YWx3SjlxYkNZT21
fQ2xsRWI4TEF0aWJDTGtyYUVPRmY2cmpyMGRSUXZ1VlRIb3BJTQ==","email":"daniele.bagiotti@cr
edit-agricole.it"},"registry.redhat.io":{"auth":"fHVoYy1wb29sLTgxNGFiODI0LTgwMzctNG
JjMy1iMTA2LWUwZDQyMWY5NDU2ZjpleUpoYkdjaU9pSlNVelV4TWlKOS5leUp6ZFdJaU9pSTJNekZpWW1Ka
09XTXlOVGswWTJaak9UWm1abUkwWVRRMU4yTmhORE00TVNKOS5jdVU0TjA4R3Q5VUh6Snk0d3VXOV9aeFdT
c1FiN0dUYThWRm0yTTdqWFBmSXd3TXZ0YnZGTHVwYno5bTZZX3VXTE91UF9SZk9xSVpldGk1X3oxUnBNOFV
nRDMzUUJ2V2QxbGFxMkJEY0ZUTHlyQ2Z5anVvaGdvZFppZE5SRFgwQXRURFdDLTlOMmRlMTZMUWhaeUttYn
BaZlFDVVo5TGtDLWdQSk1xVmNTOFY3RzhXM2x0QWkyTm55TGp1dzBDMk5MUjl3M3R4M29tRnhES1Jabm1kY
mFQemdzQ2o4bnNCZXhDYmtYRFVCVWo1YUFjX1Fha3FxNVZZYmtxYTQtNHRZYTljamc3RXEtUy11dW5pWlo3
cldxLUhOdmlYRUpWVVY0M1NkdnlNZ2I0bTQwanFaYVpqOVpLQ1pycktKVUdnd0tTS1IteUNwcHhWZWZScnB
0QmZ4WndrM0ZPNGg1azZuOUdOSE1RazdmRGVnTEJ5WVdmcVdQNnZHSENudW1LRVFBLWczcXBPZENrWlptV2
VRQlpHaExHNkhpS0luRHVIOUxKb2hhSm5BcTBqVVhsVHdGYWZ4OUtoVXhUemM1cDhBUmQwZGdEd2tUZjJaV
WZKM2czVW1QUjNHaTRmY2xTaHc5RW9UbXlKXzYzdHpSV0pJd053X0VSOE9QSHVnNFNwM2pfZ2lPaXNCSmI2
TU5ybkJ3WmFXWElDNjdCbnR2REJVTXgyZkdYbDJ2cDZEamdpWjZxU2Z5blRwWXFpaFBGSWplbldQd0VqUFl
5b01nQTF2NVJoanppT1ZCemZXRTVKY1pOdC1VaU5GckdaMmV0bXdQUkpNaThJODJ2YWx3SjlxYkNZT21fQ2
xsRWI4TEF0aWJDTGtyYUVPRmY2cmpyMGRSUXZ1VlRIb3BJTQ==","email":"daniele.bagiotti@credi
t-agricole.it"}}}'
sshKey: 'ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAINXQWDylUR5IzHTI0R2eWkRHqZeIfIo7X+qjxoBrRAwW
root@grpi-ocp-hv00'
```

L'*install-config.yaml* è stato posizionato sia all'interno della directory **/root/ocp-acm** che **/root/ocp-acm/installation_dir.** L'installazione è stata lanciata con il comando seguente:

```Python
[root@grpi-ocp-hv00 ocp-acm]# cp install-config.yaml i./nstallation_dir/.
[root@grpi-ocp-hv00 ocp-acm]# openshift-install create cluster --dir
/root/ocp-acm/installation_dir --log-level  debug
....
INFO Checking to see if there is a route at openshift-console/console...
DEBUG Route found in openshift-console namespace: console
DEBUG OpenShift console route is admitted
```

```
INFO Install complete!
INFO To access the cluster as the system:admin user when using 'oc', run 'export
KUBECONFIG=/root/ocp-acm/installation_dir/auth/kubeconfig'
INFO Access the OpenShift web-console here:
https://console-openshift-console.apps.ocp-parallelo.cariprpcpar.it
INFO Login to the console with user: "kubeadmin", and password: "XXXXXXXXXXX"
DEBUG Time elapsed per stage:
DEBUG      pre-bootstrap: 38s
DEBUG          bootstrap: 12s
DEBUG             master: 17s
DEBUG Bootstrap Complete: 24m12s
DEBUG                API: 5m30s
DEBUG  Bootstrap Destroy: 1m14s
DEBUG  Cluster Operators: 18m22s
INFO Time elapsed: 45m2s
[root@grpi-ocp-hv00 ocp-acm]#
```

Al termine dell’installazione è possibile settare la variabile di ambiente KUBECONFIG per autenticarsi sul cluster appena creato:

```
Python
[root@grpi-ocp-hv00 ocp-acm]# oc export
KUBECONFIG=/root/ocp-acm/installation_dir/auth/kubeconfig
[root@grpi-ocp-hv00 ocp-acm]# oc whoami
```

In questa fase, il cluster è composto da 3 nodi master e da 3 nodi worker. Nei paragrafi seguenti verrà spiegato come tali nodi worker sono stati sostituiti dai nodi infrastrutturali.

2.2. Installazione ACM

Al termine dell’installazione minimale è stato installato l’operator “*Advanced Cluster Management for Kubernetes”* utilizzando la dashboard.

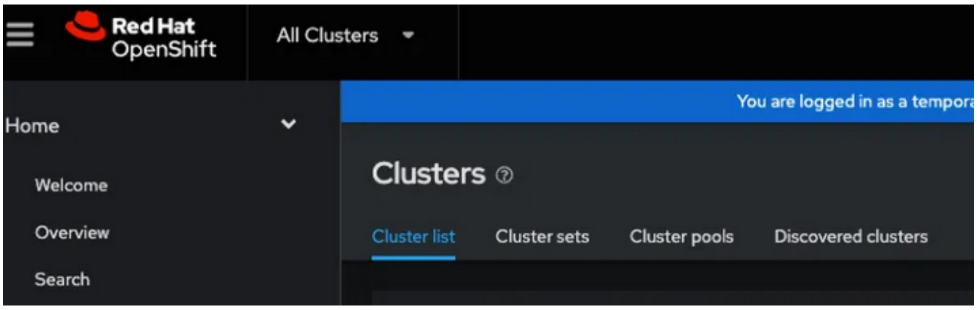
I passi eseguiti sono i seguenti:

- Collegandosi alla console di OCP del cluster HUB, all’interno del tab "Operator Hub", digitare “Advanced Cluster Management for Kubernetes” e cliccare su “install”.
- Nella pagina della subscription che si apre, lasciare il default “open-cluster-management” come namespace di default per l’installazione.
- Modalità di aggiornamento: selezionare “Automatic”.

Una volta installato l’operator, selezionarlo e modificare la strategia di aggiornamento della subscription, da “Automatic” a “Manual”.

Cliccando all’interno della sezione “MultiClusterHub” creare l’oggetto “MultiClusterHub” lasciando i valori di default.

Terminata l’installazione, è possibile collegarsi alla console di ACM utilizzando il tab “All Clusters” che si trova in alto a sinistra della console di OCP.



2.3. Configurazioni aggiuntive

Le cosiddette “operazioni di Day2”, sono state eseguite sul cluster HUB ACM utilizzando le policy di ACM.

Per semplificare la definizione e la gestione delle policy, è stato utilizzato il PolicyGenerator.

Seguono i comandi eseguiti per configurare il plugin del PolicyGenerator sul nodo bastion:

```python
[root@grpi-ocp-hv00 ocp-acm]# mkdir -p
${HOME}/.config/kustomize/plugin/policy.open-cluster-management.io/v1/policygenerat
or
[root@grpi-ocp-hv00 ~]# wget
https://github.com/open-cluster-management-io/policy-generator-plugin/releases/down
load/v1.13.0/linux-amd64-PolicyGenerator

[root@grpi-ocp-hv00 ocp-acm]# chmod +x linux-amd64-PolicyGenerator
[root@grpi-ocp-hv00 ocp-acm]# mv linux-amd64-PolicyGenerator
${HOME}/.config/kustomize/plugin/policy.open-cluster-management.io/v1/policygenerat
or/PolicyGenerator
```

All’interno della directory “**/root/ocp-acm/policy-generator/acm-hub**” sono state create le policy per il cluster ocp-parallelo, nei prossimi paragrafi verranno descritte puntualmente.

2.3.1. Servizio Chronyd

All’interno della directory **ntp-conf** sono stati definiti i template necessari a configurare il servizio *chronyd* sulle macchine virtuali di OCP.

Python

```
[root@grpi-ocp-hv00 acm-hub]# ll /root/ocp-acm/policy-generator/acm-hub/ntp-conf
-rw-r--r--. kustomization.yaml
-rw-r--r--. ntp-conf.yaml
-rw-r--r--. ntp-master-conf.yaml
-rw-r--r--. ntp-worker-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat kustomization.yaml
generators:
  - ntp-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-ntp-conf-ocp
placementBindingDefaults:
  name: placement-binding-ntp-conf-ocp
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: local-cluster
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-ntp-master-ocp
    manifests:
      - path: ntp-master-conf.yaml
  - name: policy-ntp-worker-ocp
    manifests:
      - path: ntp-worker-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-master-conf.yaml
# Generated by Butane; do not edit
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: master
  name: 99-master-custom-ntp
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            compression: gzip
                                                                            source:
data:;base64,H4sIAAAAAAAC/2TLwQ3DIAyF4bun8AQGQi8dJyEOQaUYGTdStq9a5Zbb0/v1dZGKnnTnSr
9NzTqJZizLR4fBYD1YMXiaQqTwoOCf9zNOsGrZbCuV0R2zuloWl3aVdrp/gff84mHcMZDHCGppnC1BlbwWv
Yzky8A3AAD//9ME84KXAAAA
          mode: 420
          overwrite: true
          path: /etc/chrony.conf

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-worker-conf.yaml
# Generated by Butane; do not edit
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-worker-custom-ntp
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            compression: gzip
                                                                            source:
data:;base64,H4sIAAAAAAAC/2TLwQ3DIAyF4bun8AQGQi8dJyEOQaUYGTdStq9a5Zbb0/v1dZGKnnTnSr
9NzTqJZizLR4fBYD1YMXiaQqTwoOCf9zNOsGrZbCuV0R2zuloWl3aVdrp/gff84mHcMZDHCGppnC1BlbwWv
Yzky8A3AAD//9ME84KXAAAA
          mode: 420
          overwrite: true
          path: /etc/chrony.conf
```

I file **ntp-master-conf.yaml** e **ntp-worker-conf.yaml** sono stati generati con l'utility "butane" come segue:

```
Python
[root@grpi-ocp-hv00 ~]# curl
https://mirror.openshift.com/pub/openshift-v4/clients/butane/latest/butane --output
butane
[root@grpi-ocp-hv00 ~]# chmod +x butane

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-master.bu
variant: openshift
version: 4.10.0
metadata:
  name: 99-master-custom-ntp
  labels:
    machineconfiguration.openshift.io/role: master
storage:
  files:
   - path: /etc/chrony.conf
     mode: 0644
     overwrite: true
     contents:
       inline: |
         pool 0.rhel.pool.ntp.org iburst
         server NTP IP1
         server NTP IP2
         driftfile /var/lib/chrony/drift
         makestep 1.0 3
         rtcsync
         logdir /var/log/chrony

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-worker.bu
variant: openshift
version: 4.10.0
metadata:
  name: 99-worker-custom-ntp
  labels:
    machineconfiguration.openshift.io/role: worker
storage:
  files:
   - path: /etc/chrony.conf
     mode: 0644
     overwrite: true
     contents:
       inline: |
         pool 0.rhel.pool.ntp.org iburst
         server NTP IP1
         server NTP IP2
         driftfile /var/lib/chrony/drift
         makestep 1.0 3
         rtcsync
         logdir /var/log/chrony


[root@grpi-ocp-hv00 ntp-conf]# /root/butane 99-worker-custom.bu -o
./ntp-worker-conf.yaml
[root@grpi-ocp-hv00 ntp-conf]# /root/butane 99-master-custom.bu -o
./ntp-master-conf.yaml
[root@grpi-ocp-hv00 ntp-conf]# rm -f 99-worker-custom.bu 99-master-custom.bu
```

A questo punto sono state create le policy con il comando seguente:

```
Python
[root@grpi-ocp-hv00 ntp-conf]# oc kustomize --enable-alpha-plugin=true . | oc apply
-f -
```

IMPORTANTE: la configurazione del servizio *chronyd* prevede il riavvio di tutti i nodi del cluster in maniera *rolling*. Attendere che tutti i nodi vengano riavviati prima di passare allo step successivo.

2.3.2. Definizione nodi infrastrutturali

All'interno della directory **infra-nodes** sono stati definiti i template necessari a:

- Eseguire il deploy dei nodi infrastrutturali
- Creare il *machineconfigpool* per i nodi infrastrutturali

Python

```
[root@grpi-ocp-hv00 acm-hub]# ll /root/ocp-acm/policy-generator/acm-hub/infra-nodes
-rw-r--r--. acm-hub-infra-machineset.yaml
-rw-r--r--. infra-nodes-conf.yaml
-rw-r--r--. kustomization.yaml
-rw-r--r--. mcp-infra.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat kustomization.yaml
generators:
  - infra-nodes-conf.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat infra-nodes-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-infra-node-conf-ocp
placementBindingDefaults:
  name: placement-binding-infra-node-conf-ocp
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: local-cluster
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-infra-node-machineset-ocp
    manifests:
      - path: acm-hub-infra-machineset.yaml
  - name: policy-infra-node-mcp-ocp
    manifests:
      - path: mcp-infra.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat acm-hub-infra-machineset.yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  labels:
    machine.openshift.io/cluster-api-cluster: ocp-parallelo-6lnrk
  name: ocp-parallelo-6lnrk-infra-0
  namespace: openshift-machine-api
```

```
spec:
  replicas: 3
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: ocp-parallelo-6lnrk
      machine.openshift.io/cluster-api-machineset: ocp-parallelo-6lnrk-infra-0
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: ocp-parallelo-6lnrk
        machine.openshift.io/cluster-api-machine-role: worker
        machine.openshift.io/cluster-api-machine-type: worker
        machine.openshift.io/cluster-api-machineset: ocp-parallelo-6lnrk-infra-0
    spec:
      lifecycleHooks: {}
      metadata:
        labels:
          node-role.kubernetes.io/infra: ""
      providerSpec:
        value:
          apiVersion: machine.openshift.io/v1beta1
          credentialsSecret:
            name: vsphere-cloud-credentials
          diskGiB: 120
          kind: VSphereMachineProviderSpec
          memoryMiB: 32768
          metadata:
            creationTimestamp: null
          network:
            devices:
            - networkName: dvpg_620_DMZ_ocprhel_par
          numCPUs: 16
          numCoresPerSocket: 2
          snapshot: ""
          template: ocp-parallelo-6lnrk-rhcos-generated-region-generated-zone
          userDataSecret:
            name: worker-user-data
          workspace:
            datacenter: ACILIA
            datastore: /ACILIA/datastore/ESX-OCP-PREPROD-AC-0000
            folder: /ACILIA/vm/PARALLELO/OCP
            resourcePool: /ACILIA/host/OCP_PREPROD//Resources
            server: ac-cags-vcsa001.cariprpc.it


[root@grpi-ocp-hv00 infra-nodes]# cat mcp-infra.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: infra
spec:
  machineConfigSelector:
    matchExpressions:
    - key: machineconfiguration.openshift.io/role
      operator: In
      values:
      - worker
      - infra
  nodeSelector:
    matchExpressions:
    - key: node-role.kubernetes.io/infra
      operator: Exists
```

Per creare le policy è stato eseguito il seguente comando:

```
Python
[root@grpi-ocp-hv00 infra-nodes]# oc kustomize --enable-alpha-plugin=true . | oc
apply -f -
```

A questo punto è possibile verificare la creazione del *machineset* e del *machineconfigpool.*

```
Python
[root@grpi-ocp-hv00 infra-nodes]# oc get machinesets -A

KKK

[root@grpi-ocp-hv00 infra-nodes]# oc get mcp

KKK
```

IMPORTANTE: Per aumentare la numerosità dei nodi infrastrutturali, andare in edit sul template della policy *acm-hub-infra-machineset.yaml* modificando il valore "replicas" e rilanciare il comando di create della policy, questo aggiornerà la policy con il nuovo valore.

A questo punto sono stati eliminati i nodi "worker" dal cluster HUB ACM eseguendo i seguenti comandi:

```
Python
[root@grpi-ocp-hv00 infra-nodes]# oc scale --replicas=0 machineset
ocp-parallelo-6lnrk-worker-0
[root@grpi-ocp-hv00 infra-nodes]# oc delete machineset ocp-parallelo-6lnrk-worker-0
```

2.3.3. Autenticazione tramite LDAP

All’interno della directory **oauth** sono stati definiti i template necessari a:

- Creare la *configmap* contenente la CA per l’utilizzo del protocollo ldaps nella comunicazione con il server LDAP
- Creare la secret contenente l’utenza per eseguire il bind all’LDAP e la password
- Configurare come metodo di autenticazione sul cluster, l’LDAP di Crédit Agricole

Python

```
[root@grpi-ocp-hv00 acm-hub]# ll /root/ocp-acm/policy-generator/acm-hub/oauth
-rw-r--r--. auth-conf.yaml
-rw-r--r--. bind-secret.yaml
-rw-r--r--. kustomization.yaml
-rw-r--r--. cm-ca.yaml
-rw-r--r--. oauth.yaml

[root@grpi-ocp-hv00 oauth]# cat kustomization.yaml
generators:
  - auth-conf.yaml

[root@grpi-ocp-hv00 oauth]# cat auth-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-auth-conf-ocp
placementBindingDefaults:
  name: placement-binding-auth-conf-ocp
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: local-cluster
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-auth-conf-ocp
    manifests:
      - path: oauth.yaml
  - name: policy-auth-cm-ca-ocp
    manifests:
      - path: cm-ca.yaml
  - name: policy-auth-bind-secret-ocp
    manifests:
      - path: bind-secret.yaml

[root@grpi-ocp-hv00 oauth]# cat bind-secret.yaml
apiVersion: v1
data:
  bindPassword: V004VEdTMjVXSjEzUXphMjEkUFI=
kind: Secret
```

```
metadata:
  name: ldap-secret
  namespace: openshift-config
type: Opaque

[root@grpi-ocp-hv00 oauth]# cat cm-ca.yaml
apiVersion: v1
data:
  ca.crt: |+
    -----BEGIN CERTIFICATE-----
    MIIFKjCCAxKgAwIBAgIQOLXqjbUkq5dN85ulGnvLPTANBgkqhkiG9w0BAQsFADAm
    MSQwIgYDVQQDExtDcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1QQVIwHhcNMTcwNTAy
    MTU0NDMxWhcNMzcwNTAyMTU1NDMwWjAmMSQwIgYDVQQDExtDcmVkaXRBZ3JpY29s
    ZUl0YWxpYVJDQS1QQVIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCh
    6zrpKWzle9HixD8Awnq0TnDC3tiDcv009WuWT5qb0PylqHmhjHy06vywNxV12OlV
    +GqWOfvxfJrf3+nWLir7nLxmf05732stWnK2ZK4hS4zaLkG/vt4IKZqkQSal3i1/
    /Ad1Pps8KbDXdgxZME1AxkBM6EbNU1RGoxjT/0xddbfJzZ7Ol5k4rsalM5vqIKfd
    bFBmyrtC7//YabRiUqYi19ulFFCXb4Wf4nu0rMwRhKynPrm+TooiSvDIyb0qEzIS
    3nOxn0ZjvUuL78AyikGWf70ay6tBol2OJTLCWc30tQPNK2CGznjdk45u24bV/X1F
    pGDq8XbdDDP8jnIMX/S/d4ABKcjOmL/cV1oNm5SfrI+E53EXyqW/rJnx40csWKwj
    nFoItg8KUNEC9cgRR/7u/4OVHIiX065mqKef1HNHQGeNlqFPKEMqdWXDYLljw380
    6g9VF4Wxq40JRN2QyzW++GpMAK88WfsxTbXx5GJ8mA1G/Zm/glPFniZGMDlx1IxS
    jfZ/mXPTDdmact0PwCBT45P7EWcbdosFrnHf5qCo6z8QAUMJv0zlSN6orPOAWald
    fZmpRfhyoQh+DeQ+IoTZ27E/mLm7lLkX1Ixj7Y+sQaAdQ3AjBtHyYgzmPYiI0TJO
    3h63mZWrHXu22tqlTufSmZnQvHxGgiQ14Ruqv0NQIQIDAQABo1QwUjALBgNVHQ8E
    BAMCAYYwEgYDVR0TAQH/BAgwBgEB/wIBATAdBgNVHQ4EFgQUN1a2wutAq3+PW3n2
    AFnJxV7iTUEwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggIBAB7t
    opTXqZhxm+3Fkg3vRoVozBqD1cPZ/NNFE70yKe+vsVXYg+QLfXZE24Uo0CYp/oRZ
    9fJ2t80wIQ0KU2RPZq9Bpi6H37vkV5b6UI55SQZaLwCJfNHkouMqWVH6InfLVF2K
    ARuPTEl33CvDN6sB+PT9IgUZtgpdjj/cCcMZS7v8LmDLFJlFmosEPnu2nTnadfVg
    knlQ//cTiWHWM8ELyK3VnEDXHQqrFWSvjbd8trVi6pYP/aV07a1GWRctryJZGms7
    yMVpW3q4dDK+kd0CerXurdsKuMJkzrcsqD73iPpZiGgilsj2N3iuBm99vwd93HVl
    ha1Lvr1ZCkCL1f2J7iffxk9Wrm1GauFaO25ZydJ5UXu4ihgbnk6AYSK9h19IRc1r
    PmLIghzpqLRXJpZjUa1b6Hytl0jookPbHPb0M6cCK35+L+fdetGXiLSZn4Y1vtqe
    4rjHKa68Lkk4S+ljwz5DvbouCcHAgvOxTkX0M5fkClKS1E7gp2Eu3F8o31dmBlci
    0kZQvFwHFdSNj3zIkxtoRE3TQD2I5CTzMkiURBD264ISjdwc8uKNHadILn1GyaXJ
    lbNvnKb6w7hrcXCqHnTvl1mXu0MlX5zF+h+5mrpGezfEJuK7AlWyj/NsiMVjrVb2
    TaSm5to8Jz08SkHyz2J5baoH0yx0g+AJKxRtnwqt
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    MIIILDCCBhSgAwIBAgITKgAAAANLM56OzEXAcwAAAAAAAzANBgkqhkiG9w0BAQsF
    ADAmMSQwIgYDVQQDExtDcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1QQVIwHhcNMTcw
    NTAzMDkyODU5WhcNMjcwNTAzMDkzODU5WjBXMRIwEAYKCZImiZPyLGQBGRYCaXQx
    GzAZBgoJkiaJk/IsZAEZFgtjYXJpcHJwY3BhcjEkMCIGA1UEAxMbQ3JlZGl0QWdy
    aWNvbGVJdGFsaWFTQ0EtUEFSMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
    AgEAqtmT+HRBlIEG66OzYTzRENNO4Y2LW2CYyGpMIMHzpoAgTtRHQC1JbcKHE/+3
    gyijkipPkbuYbrLea3zMbSgsJHwVasflXK+NufVE1412CFBoLBUUAEivh2zpBkmM
    gOpYo/SvjGwCUuN7vVbraMGbflvDi27iKfMZgzK7hMNNO/ew+MNMqIVq/p95UC3L
    Fx2TJtF6+pUEL1Tm06sWTniLk9PhL0s2re17U/mhz+QrGLsbqom4Zi+LrKB84TX0
    Lis2iSCIIUT4piRccZDh3BF2TOkYrVlPFv1H3+bOpilzZVsSogzWy7I9sP/kDcqv
    K3y2cLHRsckeQcuempJUj5bX+l6F9uDw80gMoBGRi/y2SF7doWQvoHuE2TTLRr0W
    GAbGu2yy5GSO9i5l5i7sdouwi0MEhaYIsEvif68Q3Ja99PLjx1LvDcuIUKBu7hgm
    uXuXkhMFUVjh8PdSIINpzG8wSPILpQC5uH3n6rGBCEBkqRjdmmLWADdgseU6ESMp
    wT3ViDxSAg3zvWMF1v/H6hnOuBspnDGnUEbuY1JQjQP/aWn9+lfd8PGLem5S5DKL
    Gb4vvWsw36tgoJpFQ6TqyV70z/hLMy8GFeWuOn8aU6NFAyzn56sPGY05KLwjDG+i
    XuauPrl9pIvskvsJ69AkawbS6c2+fk1yBJw97g75EAuJsk8CAwEAAaOCAyAwggMc
    MBIGCSsGAQQBgjcVAQQFAgMBAAEwIwYJKwYBBAGCNxUCBBYEFFnklte59RhxVuJM
    auvEP4SuWNcHMB0GA1UdDgQWBBShy+zN34OTBRtsC41QwKHlT3KY5zAZBgkrBgEE
    AYI3FAIEDB4KAFMAdQBiAEMAQTALBgNVHQ8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB
    /wIBADAfBgNVHSMEGDAWgBQ3VrbC60Crf49befYAWcnFXuJNQTCCAS0GA1UdHwSC
    ASQwggEgMIIBHKCCARigggEUhoHLbGRhcDovLy9DTj1DcmVkaXRBZ3JpY29sZUl0
    YWxpYVJDQS1QQVIsQ049R1JQSS1DQUEtSFYzMSxDTj1DRFAsQ049UHVibGljJTIw
    S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1D
    QVJJUFJQQ1BBUixEQz1pdD9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/
    b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGRGh0dHA6Ly9wa2kuY2Fy
    aXBycGNwYXIuaXQvQ2VydEVucm9sbC9DcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1Q
    QVIuY3JsMIIBMgYIKwYBBQUHAQEEggEkMIIBIDCBvQYIKwYBBQUHMAKGgbBsZGFw
    Oi8vL0NOPUNyZWRpdEFncmljb2xlSXRhbGlhUkNBLVBBUixDTj1BSUEsQ049UHVi
    bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
    bixEQz1DQVJJUFJQQ1BBUixEQz1pdD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0
    Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTBeBggrBgEFBQcwAoZSaHR0cDov
    L3BraS5jYXJpcHJwY3Bhci5pdC9DZXJ0RW5yb2xsL0dSUEktQ0FBLUhWMzFfQ3Jl
    ZGl0QWdyaWNvbGVJdGFsaWFSQ0EtUEFSLmNydDANBgkqhkiG9w0BAQsFAAOCAgEA
    XbBUDlc4FeCJGdJeWWDvgK2brxO9VshgjgZV9GGmmFlLR/TKim0VkrRAjfSvxf1x
    nto8bHZ2ivxBr0RSBVOXEvVYycMIkMxpbGbKAIkN2PnuMO5FCudNYpMA4P0HcQch
    wiGQlonj7e2/Azvtyc5ML4xLubb6JQNt1L/76dCdheGmdYj3YNkrIzaDkMe3jZmW
    TrVI+hOLOL9XuOnNzQkhZ0INQ/QQmUGQ6xdaM1z5MVkOvTPpkzhD8s6Vt/nkodOA
    J9gQEDlhO46tl67QqplsA8jX3wgRqvffZ3E9ZSx3t1dDsnslhsZEoDHVALTMcyfU
    EMEsGtRlkWPrUcEPzBnn9mTegaoEAby53OAVaW5FeT2iGSlCIhukiu70Mvf8MIAA
    /p3kDl2J3OtUJ/THjg8952JCa8WBpvON25cV4QU0PhfJmnBfoVHYmpAntcXcECS1
    OHJnkD0pRgqKz+GcW7mIVWrygaXwH+nXrJw22ympf+s2h3xvjPqFCy5PxDjZIyaP
    OD2S8PIWHfQZTztYhhsTl675U6oGO3T5/BRxQ+s+AKtjUpQ24Wz52tdulD9Ya1Xc
    f6Msid7qH9Nv9lT5sjyy+bNdla2YFvXcjEIh7g8GVqRWszkbbb2irU0f5PbjiApV
    Yv4sy+JZ53ZzY07YmIHBlvFPlm4194MNTBgbpd+zBHE=
    -----END CERTIFICATE-----
kind: ConfigMap
metadata:
  name: ca-config-map
  namespace: openshift-config

[root@grpi-ocp-hv00 oauth]# cat oauth.yaml
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
  - ldap:
      attributes:
        email:
        - mail
        id:
        - dn
        name:
        - cn
        preferredUsername:
        - sAMAccountName
      bindDN:
CN=cp_4462_ocp_ldap,OU=OU-UTENTI-SERVIZI,OU=OU-UTENTI,DC=cariprpcpar,DC=it
      bindPassword:
        name: ldap-secret
      ca:
        name: ca-config-map
      insecure: false
      url:
ldaps://msad0par.cariprpcpar.it/DC=cariprpcpar,DC=it?sAMAccountName?sub?(&(objectCl
ass=user)(|(memberOf=CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_DTR_USER,CN=User
s,DC=cariprpcpar,DC=it)(memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it)(mem
berOf=CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it)))
    mappingMethod: claim
    name: ldap
    type: LDAP
```

Per configurare l'operator dell'autenticazione è necessario eseguire il seguente comando:

Python

```
[root@grpi-ocp-hv00 oauth]# oc kustomize --enable-alpha-plugin=true . | oc apply -f
-
```

Attendere il riavvio dei pod dell'autenticazione prima di testare la login tramite LDAP.

2.3.4. Sync gruppi di utenti tra alberatura LDAP e OCP

All'interno della directory **group-sync-operator** sono stati definiti i template necessari a:

- Creare il namespace che ospita il group-sync-operator
- Installare il group-sync-operator
- Creare la *configmap* contenente la CA per l'utilizzo del protocollo ldaps nella comunicazione con il server LDAP: il campo ca.crt contiene il *base64encode* della CA.
- Creare la secret contenente l'utenza per eseguire il bind all'LDAP e la password
- Configurare il group sync operator
- Associare il ruolo cluster-admin agli utenti appartenenti al gruppo CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it

Python

```
[root@grpi-ocp-hv00 acm-hub]# ll
/root/ocp-acm/policy-generator/acm-hub/group-sync-operator
-rw-r--r--. group-sync-conf.yaml
-rw-r--r--. ldap-ca-bundle-group-sync.yaml
-rw-r--r--. ldap-creds-group-sync.yaml
-rw-r--r--. ldap-groupsync.yaml
-rw-r--r--. namespace.yaml
-rw-r--r--. operatorgroup.yaml
-rw-r--r--. role-bindig.yaml
-rw-r--r--. subscription.yaml
```

```
-rw-r--r--. kustomization.yaml


[root@grpi-ocp-hv00 group-sync-operator]# cat kustomization.yaml
generators:
  - group-sync-conf.yaml
[root@grpi-ocp-hv00 group-sync-operator]# cat group-sync-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-group-sync-conf-ocp
placementBindingDefaults:
  name: placement-binding-group-sync-conf-ocp
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: local-cluster
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-group-sync-namespace-ocp
    manifests:
      - path: namespace.yaml
  - name: policy-group-sync-operatorgroup-ocp
    manifests:
      - path: operatorgroup.yaml
  - name: policy-group-sync-subscription-ocp
    manifests:
      - path: subscription.yaml
  - name: policy-group-sync-ldap-groupsync-ocp
    manifests:
      - path: ldap-groupsync.yaml
  - name: policy-group-sync-ca-secret-ocp
    manifests:
      - path: ldap-ca-bundle-group-sync.yaml
  - name: policy-group-sync-bind-secret-ocp
    manifests:
      - path: ldap-creds-group-sync.yaml
  - name: policy-group-sync-admin-ocp
    manifests:
      - path: role-bindig.yaml

[root@grpi-ocp-hv00 group-sync-operator]# cat namespace.yaml
apiVersion: v1
kind: Namespace
metadata:
  name: group-sync-operator
spec:
  finalizers:
  - kubernetes
[root@grpi-ocp-hv00 group-sync-operator]# cat operatorgroup.yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: group-sync-operator
  namespace: group-sync-operator
spec:
  targetNamespaces:
  - group-sync-operator
[root@grpi-ocp-hv00 group-sync-operator]# cat subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: group-sync-operator
  namespace: group-sync-operator
spec:
  channel: alpha
  installPlanApproval: Manual
  name: group-sync-operator
  source: community-operators
  sourceNamespace: openshift-marketplace

[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-groupsync.yaml
apiVersion: redhatcop.redhat.io/v1alpha1
kind: GroupSync
metadata:
  name: ldap-groupsync
  namespace: group-sync-operator
spec:
  providers:
  - ldap:
      activeDirectory:
        groupMembershipAttributes:
        - memberOf
        userNameAttributes:
        - sAMAccountName
        usersQuery:
          baseDN: DC=cariprpcpar,DC=it
          derefAliases: never
          filter:
(&(objectClass=user)(|(memberOf=CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_DTR_U
SER,CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar
,DC=it)(memberOf=CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it)))
          pageSize: 0
          scope: sub
      caSecret:
        kind: Secret
        name: ldap-ca-bundle-group-sync
        namespace: group-sync-operator
      credentialsSecret:
        kind: Secret
        name: ldap-creds-group-sync
        namespace: group-sync-operator
      insecure: false
      url: ldaps://msad0par.cariprpcpar.it
      whitelist:
      - CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_DTR_USER,CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it
    name: ldap-group-sync
  schedule: '*/5 * * * *'
```

```
[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-ca-bundle-group-sync.yaml
apiVersion: v1
data:
  ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZLakNDQXhLZ0F3SUJBZ0lRT0xYcWpiVWtxNWROODV
1bEdudkxQVEFOQmdrcWhraUc5dzBCQVFzRkFEQW0KTVNRd0lnWURWUVFERXh0RGNtVmthWFJCWjNKcFkyOX
NaVWwwWVd4cFlWSkRRUzFRUVZJd0hoY05NVGN3TlRBeQpNVFUwTkRNeFdoY05NemN3TlRBeU1UVTFORE13V
2pBbU1TUXdJZ1lEVlFRREV4dERjbVZrYVhSQlozSnBZMjlzClpVbDBZV3hwWVZKRFFTMVFRVkl3Z2dJaU1B
MEdDU3FHU0liM0RRRUJBUVVBQTRJQ0R3QXdnZ0lLQW9JQ0FRQ2gKNnpycEtXemxlOUhpeEQ4QXducTBUbkR
DM3RpRGN2MDA5V3VXVDVxYjBQeWxxSG1oakh5MDZ2eXdOeFYxMk9sVgorR3FXT2Z2eGZKcmYzK25XTGlyN2
5MeG1mMDU3MzJzdFduSzJaSzRoUzR6YUxrRy92dDRJS1pxa1FTYWwzaTEvCi9BZDFQcHM4S2JEWGRneFpNR
TFBeGtCTTZFYk5VMVJHb3hqVC8weGRkYmZKelo3T2w1azRyc2FsTTV2cUlLZmQKYkZCbXlydEM3Ly9ZYWJS
aVVxWWkxOXVsRkZDWGI0V2Y0bnUwck13UmhLeW5Qcm0rVG9vaVN2REl5YjBxRXpJUwozbk94bjBaanZVdUw
3OEF5aWtHV2Y3MGF5NnRCb2wyT0pUTENXYzMwdFFQTksyQ0d6bmpkazQ1dTI0YlYvWDFGCnBHRHE4WGJkRE
RQOGpuSU1YL1MvZDRBQktjak9tTC9jVjFvTm01U2ZySStFNTNFWHlxVy9ySm54NDBjc1dLd2oKbkZvSXRnO
EtVTkVDOWNnUlIvN3UvNE9WSElpWDA2NW1xS2VmMUhOSFFHZU5scUZQS0VNcWRXWERZTGxqdzM4MAo2ZzlW
RjRXeHE0MEpSTjJReXpXKytHcE1BSzg4V2ZzeFRiWHg1R0o4bUExRy9abS9nbFBGbmlaR01EbHgxSXhTCmp
mWi9tWFBURGRtYWN0MFB3Q0JUNDVQN0VXY2Jkb3NGcm5IZjVxQ282ejhRQVVNSnYwemxTTjZvclBPQVdhbG
QKZlptcFJmaHlvUWgrRGVRK0lvVFoyN0UvbUxtN2xMa1gxSXhqN1krc1FhQWRRM0FqQnRIeVlnem1QWWlJM
FRKTwozaDYzbVpXckhYdTIydHFsVHVmU21ablF2SHhHZ2lRMTRSdXF2ME5RSVFJREFRQUJvMVF3VWpBTEJn
TlZIUThFCkJBTUNBWVl3RWdZRFZSMFRBUUgvQkFnd0JnRUIvd0lCQVRBZEJnTlZIUTRFRmdRVU4xYTJ3dXR
BcTMrUFczbjIKQUZuSnhWN2lUVUV3RUFZSkt3WUJCQUdDTnhVQkJBTUNBUUF3RFFZSktvWklodmNOQVFFTE
JRQURnZ0lCQUI3dApvcFRYcVpoeG0rM0ZrZzN2Um9Wb3pCcUQxY1BaL05ORkU3MHlLZSt2c1ZYWWcrUUxmW
FpFMjRVbzBDWXAvb1JaCjlmSjJ0ODB3SVEwS1UyUlBacTlCcGk2SDM3dmtWNWI2VUk1NVNRWmFMd0NKZk5I
a291TXFXVkg2SW5mTFZGMksKQVJ1UFRFbDMzQ3ZETjZzQitQVDlJZ1VadGdwZGpqL2NDY01aUzd2OExtREx
GSmxGbW9zRVBudTJuVG5hZGZWZwprbmxRLy9jVGlXSFdNOEVMeUszVm5FRFhIUXFyRldTdmpiZDh0clZpNn
BZUC9hVjA3YTFHV1JjdHJ5SlpHbXM3CnlNVnBXM3E0ZERLK2tMENlclh1cmRzS3VNSmt6cmNzcUQ3M2lQc
FppR2dpbHNqMk4zaXVCbTk5dndkOTNIVmwKaGExTHZyMVpDa0NMMWYySjdpZmZ4azlXcm0xR2F1RmFPMjVa
eWRKNVVYdTRpaGdibms2QVlTSzloMTlJUmMxcgpQbUxJZ2h6cHFMUlhKcFpqVWExYjZIeXRsMGpvb2tQYkh
QYjBNNmNDSzM1K0wrZmRldEdYaUxTWm40WTF2dHFlCjRyakhLYTY4TGtrNFMrbGp3ejVEdmJvdUNjSEFndk
94VGtYME01ZmtDbEtTMUU3Z3AyRXUzRjhvMzFkbUJsY2kKMGtaUXZGd0hGZFNOajN6SWt4dG9SRTNUUUQyS
TVDVHpNa2lVUkJEMjY0SVNqZHdjOHVLTkhhZElMbjFHeWFYSgpsYk52bktiNnc3aHJjWENxSG5UdmwxbVh1
ME1sWDV6RitoKzVtcnBHZXpmRUp1SzdBbFd5ai9Oc2lNVmpyVmIyClRhU201dG84SnowOFNrSHl6Mko1YmF
vSDB5eDBnK0FKS3hSdG53cXQKLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQotLS0tLUJFR0lOIENFUlRJRk
lDQVRFLS0tLS0KTUlJSUxEQ0NCaFNnQXdJQkFnSVRLZ0FBQUFOTE01Nk96RVhBY3dBQUFBQUFBekFOQmdrc
WhraUc5dzBCQVFzRgpBREFtTVNRd0lnWURWUVFERXh0RGNtVmthWFJCWjNKcFkyOXNaVWwwWVd4cFlWSkRR
UzFRUVZJd0hoY05NVGN3Ck5UQXpNRGt5T0RVNVdoY05NamN3TlRBek1Ea3pPRFU1V2pCWE1SSXdFQVlLQ1p
JbWlaUHlMR1FCR1JZQ2FYUXgKR3pBWkJnb0praWFKay9Jc1pBRVpGZ3RqWVhKcGNGNISndZM0JoY2pwFa01DSU
dBMVVFQXhNYlEzSmxaR2wwUVdkeQphV052052YkdWSmRHRnNhV0ZUUTBFdFVFRlNNSUlDSWpBTkJna3Foa2lHO
XcwQkFRRUZBQU9DQWc4QU1JSUNDZ0tDCkFnRUFxdG1UK0hSQmxJRUc2Nk96WVR6UkVOTk80WTJMVzJDWXlH
cE1JTUh6cG9BZ1R0UkhRQzFKYmNLSEUvKzMKZ3lpamtpcFBrYnVZYnJMZWEzek1iU2dzSkh3VmFzZmxYSyt
OdWZWRTE0MTJDRkJvTEJVVUFFaXZoMnpwQmttTQpnT3BZby9TdmpHd0NVdU43dlZicmFNR2JmbHZEaTI3aU
tmTVpneks3aE1OTk8vZXcrTU5NcUlWcS9wOTVVQzNMCkZ4MlRKdEY2K3BVRUwxVG0wNnNXVG5pTGs5UGhMM
HMycmUxN1UvbWh6K1FyR0xxzYnFvbTRaaStMcktCODRUWDAKTGlzMmlTQ0lJVVQ0cGlSY2NaRGgzQkYyVE9y
WXJWbFBGdjFIMytiT3BpbHpaVnNTb2d6V3k3STlzUC9yRGNxdgpLM3kyY0xIUnNja2VRY3VlbXBKVWo1Ylg
rbDZGOXVEdzgwZ01vQkdSaS95MlNGN2RvV1F2b0h1RTJUVExScjBXCkdBYkd1Mnl5NUdTTzlpNWw1aTdzZG
91d2kwTUVoYVlJc0V2aWY2OFEzSmE5OVBBangTHZEY3VJVUtCdTdoZ20KdVh1WGtoTUZVVmpoOFBkU0lJT
nB6Rzh3U1BJTHBRQzV1SDNuNnJHQkNFQmtxUmpkbW1MV0FEZGdzZVU2RVNNcAp3VDNWaUR4U0FnM3p2V01G
MXYvSDZobk91QnNwbkRHblVFYnVZMUpRalFQL2FXbjkrbGZkOFBHTGVtNVM1REtMCkdkiNHZ2V3N3MzZ0Z29
KcEZRNlRxeVY3MHovaExxNeThHRmVXdU9uOGFVNk5GQXl6bjU2c1BHWTA1S0x3akRHK2kKWHVhdVBybDlwSX
Zza3ZzSjY5QWthd2JTNmMyK2ZrMXlCSnc5N2c3NUVBdUpzazhDQXdFQUFhT0NBeUF3ZGdNYwpNQklHQ1NzR
0FRUUJnamNWQVFRRkFnTUJBQUV3SXdZSkt3WUJCQUdDTnhVQ0JCWUVGRm5rbHRlNTlSaHhWdUpNCmF1dkVQ
NFN1V05jSE1CMEdBMVVkRGdRV0JCU2h5K3pOMzRPVEJSdHNDNDFRd0tIbFQzS1k1ekFaQmdrckJnRUUKQVl
JM0ZBSUVEQjRLQUZNQWRRQmlBRU1BUVRBTEJnTlZIUThFQkFNQ0FZWXdFZ1lEVlIwVEFRSC9CQWd3QmdFQg
ovd0lCQURBZkJnTlZIU01FR0RBV2dCUTNWcmJDNjBDcmY0OWJlZllBV2NuRlh1Sk5RVENQMWR0ExVWRId
1NDkFTUXdnZ0VnTUlJQkhLQ0NBUUmlnZ2dFVWhvSExiR1JoY0Rvdkx5OURUajFEY21Wa2FYUkJaM0pwWTI5
```

```
c1pVbDAKWVd4cFlWSkRRUzFRUVZJc1EwNDlSMUpRU1MxRFFVRXRTRll6TVN4RFRqMURSRkFzUTA0OVVIVml
iR2xqSlRJdwpTMlY1SlRJd1UyVnlkbWxqWlhNc1EwNDlVMlZ5ZG1salpYTXNRMDQ5UTI5dVptbG5kWEpoZE
dsdmJpeEVRejFEClFWSkpVRkpRUTFCQlVpeEVRejFwZEQ5alpYSjBhV1pwWTJGMFpWSmxkbTlqWVhScGIyN
U1hWE4wUDJKaGMyVS8KYjJKcVpXTjBRMnhoYzNNOVkxSk1SR2x6ZEhKcFluVjBhVzl1VUc5cGJuU0dSR2gw
ZEhBNkx5OXdhMmt1WTJGeQphWEJ5Y0dOd1lYSXVhWFF2UTJWeWRFVnVjbTlzYkM5RGNtVmthWFJCWjNKcFk
yOXNaVWwwWVd4cFlWSkRRUzFRClFWSXVZM0pzTUlJQk1nWUlLd1lCQlFVSEFRRUVVnZ0VrTUlJQklEQ0J2UV
lJS3dZQkJRVUhNQUtHZ2JCc1pHRncKT2k4dkwwTk9QVU55WldScGRFRm5jbWxqYjJ4bFNYUmhiR2xoVWtOQ
kxWQkJVaXhEVGoxQlNVRXNRMDQ5VUhWaQpiR2xqSlRJd1MyVjVKVEl3VTJWeWRtbGpaWE1zUTA0OVUyVnlk
bWxqWlhNc1EwNDlRMjl1Wm1sbmRYSmhkR2x2CmJpeEVRejFEUVZKSlVGSlFRMUJCVWl4RVF6MXBkRDlqUVV
ObGNuUnBabWxqWVhSbFAySmhjMlUvYjJKcVpXTjAKUTJ4aGMzTTlZMlZ5ZEdsbWFXTmhkR2x2YmtGMWRHaH
ZjbWwwZVRCZUJnZ3JCZ0VGQlFjd0FvWlNhSFIwY0RvdgpMM0JyYVM1allYSnBjSEp3WTNCaGNpNXBkQzlEEW
lhKMFJXNXliMnhzTDBkU1VFa3RRMEZCTFVoV016RmZRM0psClpHbDBRV2R5YVdOdmJHVkpkR0ZzYVdGU1Ew
RXRVRUZTTG1OeWREQU5CZ2txaGtpRzl3MEJBUXNGQUFPQ0FnRUEKWGJCVURsYzRGZUNKR2RKZVdXRHZnSzJ
icnhPOVZzaGdqZ1pWOUdHbW1GbExSL1RLaW0wVmtyUkFqZlN2eGYxeApudG84YkhaMml2eEJyMFJTQlZPWE
V2Vll5Y01Ja014cGJHYktBSWtOMlBudU1PNUZDdWROWXBNQTRQMEhjUWNoCndpR1Fsb25qN2UyL0F6dnR5Y
zVNTDR4THViYjZKUU50MUwvNzZkQ2RoZUdtZFlqM1lOa3JJemFEa01lM2pabVcKVHJWSStoT0xPTDlYdU9u
TnpRa2haMElOUS9RUW1VR1E2eGRhTTF6NU1Wa092VFBwa3poRDhzNlZ0L25rb2RPQQpKOWdRRURsaE80NnR
sNjdRcXBsc0E4algzd2dScXZmZlozRTlaU3gzdDFkRHNuc2xoc1pFb0RIVkFMVE1jeWZVCkVNRXNHdFJsa1
dQclVjRVB6Qm5uOW1UZWdhb0VBYnk1M09BVmFXNUZlVDJpR1NsQ0lodWtpdTcwTXZmOE1JQUEKL3Aza0RsM
kozT3RVSi9USGpnODk1MkpDYThXQnB2T04yNWNWNFFVMFBoZkptbkJmb1ZIWW1wQW50Y1hjRUNTMQpPSEpu
a0QwcFJncUt6K0djVzdtSVZXcnlnYVh3SCtuWHJKdzIyeW1wZitzMmgzeHZqUHFGQ3k1UHhEalpJeWFQCk9
EMlM4UElXSGZRWlR6dFloaHNUbDY3NVU2b0dPM1Q1L0JSeFErcytBS3RqVXBRMjRXejUydGR1bEQ5WWExWG
MKZjZNc2lkN3FIOU52OWxUNXNqeXkrYk5kbGEyWUZ2WGNqRUloN2c4R1ZxUldzemtiYmIyaXJVMGY1UGJqa
UFwVgpZdjRzeStKWjUzWnpZMDdZbUlIQmx2RlBsbTQxOTRNTlRCZ2JwZCt6QkhFPQotLS0tLUVORCBDRVJU
SUZJQ0FURS0tLS0tCg==
kind: Secret
metadata:
  name: ldap-ca-bundle-group-sync
  namespace: group-sync-operator
type: Opaque

[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-creds-group-sync.yaml
apiVersion: v1
data:
  password: V004VEdTMjVXSjEzUXphMjEkUFI=
                                                                           username:
Q049Y3BfNDQ2Ml9vY3BfbGRhcCxPVT1PVS1VVEVOVEktU0VSVklaSSxPVT1PVS1VVEVOVEksREM9Y2FyaXB
ycGNwYXIsREM9aXQ=
kind: Secret
metadata:
  name: ldap-creds-group-sync
  namespace: group-sync-operator
type: Opaque

[root@grpi-ocp-hv00 group-sync-operator]# cat role-bindig.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: clusteradmin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it
```

Per creare questa policy è stato lanciato il comando seguente:

Python

```
[root@grpi-ocp-hv00 group-sync-operator]# oc kustomize --enable-alpha-plugin=true .
| oc apply -f -
```

IMPORTANTE: una volta creata la policy, collegarsi alla console di OCP, ed approvare a mano l'installation-plan dell'operator group-sync-operator.

3. Cluster di Acilia

3.1. Installazione cluster base

Il cluster di Acilia è composto dei seguenti nodi:

Ruolo	vCPU	RAM	OS disk	Count	Additional DISK size
Master	16	32	120 GB	3	
Infra	16	32	120 GB	3	
Storage	16	32	120 GB	3	1 TB
Worker	16	32	120 GB	3	

Il cluster **ocp1-parallelo** è stato installato utilizzando ACM.

All'interno della directory di lavoro, è stata creata la directory **/roo/ocp-acm/cluster-template** per posizionare i template utilizzati per la creazione del cluster **ocp1-parallelo**.

Il deploy del cluster tramite template ACM utilizza i template contenuti all'interno delle directory:

- ocp1-parallelo-namespace: primi template da utilizzare per eseguire il deploy del namespace "ocp1-parallelo" sul cluster HUB ACM.
- ocp1-parallelo-template: template da utilizzare una volta disponibile il namespace.

Python

```
[root@grpi-ocp-hv00 ocp1-parallelo-namepsace]# ll
-rw-r--r--. kustomization.yaml
-rw-r--r--. namespace.yaml

[root@grpi-ocp-hv00 ocp1-parallelo-namepsace]# cat kustomization.yaml
namespace: ocp1-parallelo
resources:
- namespace.yaml
generatorOptions:
  disableNameSuffixHash: true

[root@grpi-ocp-hv00 ocp1-parallelo-namepsace]# cat namespace.yaml
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  name: ocp1-parallelo
spec:
  finalizers:
  - kubernetes
```

Per utilizzare questi template eseguire i comandi seguenti:

Python

```
[root@grpi-ocp-hv00 ~]# cd /root/ocp-acm/deploy-cluster
[root@grpi-ocp-hv00 deploy-cluster]# oc apply -k ./ocp1-parallelo-namespace/
```

A questo punto abbiamo collezionato tutte le informazioni necessarie ad eseguire il deploy di un cluster, che riporto brevemente:

- Proxy da utilizzare
- Dimensionamento nodi master, worker, storage, infra
- Indirizzamento reti (MachineNetwork -clusterNetwork - serviceNetwork)
- Pull secret
- Informazioni sulla piattaforma sottostante:
    - nome vCenter
    - Username utenza per comunicare con API del vCenter
    - Password dell’utenza
    - Datacenter che ospita il cluster
    - defaultDatastore
    - Cluster che ospita il cluster
    - apiVIP: indirizzo IP appartenente alla machineNetwork per la risoluzione dell’fqdn delle api del cluster
    - ingressVIP: indirizzo IP appartenente alla machineNetwork per la risoluzione dell’fqdn della wildicard *apps.
    - Network: nome della newtork lato vcenter
    - Folder all’interno della quale vengono create le macchine OCP

Queste informazioni sono state riportate all’interno dei template seguenti:

Python

```
[root@grpi-ocp-hv00 ocp1-parallelo-template]# ll
-rw-r--r--  clusterdeployment.yaml
-rw-r--r--. clusterimageset.yaml
-rw-------. install-config.yaml
-rw-r--r--. klusterlet.yaml
-rw-r--r--. kustomization.yaml
-rw-r--r--. machinepool-infra.yaml
-rw-r--r--. machinepool-odf.yaml
-rw-r--r--. managedcluster.yaml
-rw-r--r--. pull-secret.txt
-rw-r--r--. secret-certs.yaml
-rw-r--r--. secret-creds.yaml
-rw-r--r--. ssh-key.txt
-rw-r--r--. ssh-pub-key.txt

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat kustomization.yaml
resources:
- clusterimageset.yaml
- klusterlet.yaml
- secret-certs.yaml
- secret-creds.yaml
- clusterdeployment.yaml
- machinepool-infra.yaml
- machinepool-odf.yaml
- managedcluster.yaml
secretGenerator:
- name: ocp1-parallelo-install-config
  namespace: ocp1-parallelo
  files:
  - ./install-config.yaml
- name: ocp1-parallelo-pull-secret
  namespace: ocp1-parallelo
  files:
  - .dockerconfigjson=./pull-secret.txt
- name: ocp1-parallelo-ssh-private-key
  namespace: ocp1-parallelo
  files:
  - ssh-publickey=./ssh-pub-key.txt
  - ssh-privatekey=./ssh-key.txt
generatorOptions:
  disableNameSuffixHash: true

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat clusterimageset.yaml
apiVersion: hive.openshift.io/v1
kind: ClusterImageSet
metadata:
  labels:
    visible: "true"
  name: img4.14.2-x86-64
spec:
  releaseImage: quay.io/openshift-release-dev/ocp-release:4.14.2-x86_64
```

```
[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat klusterlet.yaml
apiVersion: agent.open-cluster-management.io/v1
kind: KlusterletAddonConfig
metadata:
  name: 'ocp1-parallelo'
  namespace: 'ocp1-parallelo'
spec:
  clusterName: 'ocp1-parallelo'
  clusterNamespace: 'ocp1-parallelo'
  clusterLabels:
    cloud: vSphere
    vendor: OpenShift
  applicationManager:
    proxyPolicy: OCPGlobalProxy
    enabled: true
  policyController:
    proxyPolicy: OCPGlobalProxy
    enabled: true
  searchCollector:
    proxyPolicy: OCPGlobalProxy
    enabled: true
  certPolicyController:
    proxyPolicy: OCPGlobalProxy
    enabled: true
  iamPolicyController:
    proxyPolicy: OCPGlobalProxy
    enabled: true

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat secret-certs.yaml
apiVersion: v1
kind: Secret
metadata:
  name: ocp1-parallelo-vsphere-certs
  namespace: ocp1-parallelo
type: Opaque
stringData:
  .cacert: |
    -----BEGIN CERTIFICATE-----
    MIIELzCCAxegAwIBAgIJANNOO7hk0LIqMA0GCSqGSIb3DQEBCwUAMIGiMQswCQYD
    VQQDDAJDQTEXMBUGCgmSJomT8ixkARkWB3ZzcGhlcmUxFTATBgoJkiaJk/IsZAEZ
    FgVsb2NhbDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExJDAiBgNV
    BAoMG1JaLUNBR1MtVkNTQTAwMS5jYXJpcHJwYy5pdDEbMBkGA1UECwwSVk13YXJl
    IEVuZ2luZWVyaW5nMB4XDTIxMTAxODA3MDkzMloXDTMxMTAxNjA3MDkzMlowgaIx
    CzAJBgNVBAMMAkNBMRcwFQYKCZImiZPyLGQBGRYHdnNwaGVyZTEVMBMGCgmSJomT
    8ixkARkWBWxvY2FsMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEk
    MCIGA1UECgwbUlotQ0FHUy1WQ1NBMDAxLmNhcmlwcnBjLml0MRswGQYDVQQLDBJW
    TXdhcmUgRW5naW5lZXJpbmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
    AQDuNx7YVMDen24N+xA4PS3HObb1G44do5pQW0vxI88Y6K9+cheLQjala5AR3lQp
    dTcVE2yKWWKYZYUWMoxGMduJmSyj9QrGLxx5n2IFeOOYM8H12rCAZKmOo0zehsLU
    ntezTxTCFxRxnZPrF6qIDHgtJyT1zOHpGA9b9ZFIO4LXilswuHokES0NtV/kc+ZQ
    28UXTGXNWj0cGFphSvc/mncSKD+NViUDr8KdH9f6n7sYMi7TaHQjUeKDQmKesNa1
    5kiVTvqBVNOcvb/hTx4yJll03OxVTNKxjaloxtckwrTD7kDkEkP2zVGyUZtSfzrH
    koXWNmV6NuNQmAuHuJMzd9ShAgMBAAGjZjBkMB0GA1UdDgQWBBRz+1zOhjdBLK0t
    7BJjGC2O44bFrTAfBgNVHREEGDAWgQ5lbWFpbEBhY21lLmNvbYcEfwAAATAOBgNV
    HQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsFAAOC
    AQEA1kiw1Arwt12SPXlPuIA4oRWccSOPWYpTfh2EfxxJPnMI6RcmU/EJ6lpYSs/e
    h/uKHgP/Ps3BdHN/QVymrWT7oGc5Ssn+xnVRi0Yyu/16lu6gSitnfvJz627jeJpm
```

```
lTr/wLisfRQc9M8E7IlYTnRZJzSdpm8Ax9Y0uKN/xHW6f9O5sb26pR5BDIjxJMMZ
ji8hjSbjZUjTxpDp371HsPSRfBWiFtJ6vLrYVFvI5UpJbXb0OP4e7AIVJsHwDX25
eYDuoVZvKy4xM8iexc5+6eJMO3gaDFsi50bU+j8TPQC2A5LER19Z5N4H9nY8UQbm
1OjO4Nw83neeEShXuXidjXCDGg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIENDCCAxygAwIBAgIJAO6Ta05bNA6iMA0GCSqGSIb3DQEBCwUAMIG1MSQwIgYD
VQQDDBthYy1jYWdzLXZjc2EwMDEuY2FyaXBycGMuaXQxFzAVBgoJkiaJk/IsZAEZ
Fgd2c3BoZXJlMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxCzAJBgNVBAYTAklUMQ0w
CwYDVQQIDARSb21hMSQwIgYDVQQKDBtBQy1DQUdTLVZDU0EwMDEuY2FyaXBycGMu
aXQxGzAZBgNVBAsMElZNd2FyZSBFbmdpbmVlcmluZzAeFw0yMzEwMTgwOTA2MTJa
Fw0zMzEwMTUwOTA2MTJaMIG1MSQwIgYDVQQDDBthYy1jYWdzLXZjc2EwMDEuY2Fy
aXBycGMuaXQxFzAVBgoJkiaJk/IsZAEZFgd2c3BoZXJlMRUwEwYKCZImiZPyLGQB
GRYFbG9jYWwxCzAJBgNVBAYTAklUMQ0wCwYDVQQIDARSb21hMSQwIgYDVQQKDBtB
Qy1DQUdTLVZDU0EwMDEuY2FyaXBycGMuaXQxGzAZBgNVBAsMElZNd2FyZSBFbmdp
bmVlcmluZzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMdS/qYH+W/w
BGMqHxFqMy3vTUYAbdEvWdbbavJ2ArK9KZ9UoO22tPwTyxzCrFODITbTq44YBkoz
G9el51hJhmZ/pV6RRaLFr9eYe1W12JtuWpfB7i4VPKeb3UAr1XIXKFv+MhvPcLxP
8Ig6HuVs3Pdz0tk6PqP6iPqEogYT4K4o8ASQBr8d8A7hCjOJ3oMhdrpcU/FEZ+8d
iddrd5tN1JERZssT5MEhr0CaM42IJzo17OKifiFWSjawdhI+lk53x6h0qmTOqCR9
uPNvmEls6oM6GyePLMZeebtmWcy5FhOA+4To8Pm2BrSCD/g0+JDTdQsS9DC4HRhl
NHTjyTTWGvsCAwEAAaNFMEMwHQYDVR0OBBYEFLeSqPvIaz96mESKt5Ra/kHpZpxp
MA4GA1UdDwEB/wQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEAMA0GCSqGSIb3DQEB
CwUAA4IBAQAGktXkZKN8JONFv/AY7BHD5CkczuqEBdpdECu0QVFq/uMKCGwerI1T
wdpQXcwiJ7yl8ZmyVjUUkITlbJ7/63TFGk8hUt/NPwGDrw8KJ9Lr3T1wSUF2zzOz
hF+5JHdeF5DXolJXN6DNplgjowxdKT9tt+JKFOyqYtLu+oEgtKehq0PSqH8PlJm8
gfDPulaZRjvgNUbl1WkFZzjnWffn3eFoEVSiMYEyqSdok3Fr+7trMGziK/Fz/uLc
zUtzK5SkC5ijRtV1eUjlr6t1gAMNc9Cj52MHRrt2SQ9U7oY5U9yAuXlmv0NhvWtL
pO81QsGF+8S6UYZpYbrFrq/jJqMgHw+J
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIELzCCAxegAwIBAgIJAM0EHYbmfpUxMA0GCSqGSIb3DQEBCwUAMIGiMQswCQYD
VQQDDAJDQTEXMBUGCgmSJomT8ixkARkWB3ZzcGhlcmUxFTATBgoJkiaJk/IsZAEZ
FgVsb2NhbDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExJDAiBgNV
BAoMG0FDLUNBR1MtVkNTQTAwMS5jYXJpcHJwYy5pdDEbMBkGA1UECwwSVk13YXJl
IEVuZ2luZWVyaW5nMB4XDTIxMTAxODA3MDIzN1oXDTMxMTAxNjA3MDIzN1owgaIx
CzAJBgNVBAMMAkNBMRcwFQYKCZImiZPyLGQBGRYHdnNwaGVyZTEVMBMGCgmSJomT
8ixkARkWBWxvY2FsMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEk
MCIGA1UECgwbQUMtQ0FHUy1WQ1NBMDAxLmNhcmlwcnBjLml0MRswGQYDVQQLDBJW
TXdhcmUgRW5naW5lZXJpbmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQDClAWWzTmrY8BsNkVJpdjvas2TllAV935KS8hkxB5aIbQTMVGz2jV6WOIFARUe
GCw7pXcNILLcUJ8fnCY46ehtZ0DtoKgvGna/FFso6LB151z5FbJAV1NFW2QKATRo
JerqE8eFoT8Ttaw5aZEJKiBH+PicN28XBORpLCEPI5uYjGJ9hFDCcz+QUQB04vjX
xLh2Z+AkmZTYTtoWbIHsW3ook9VJ8llHI+nL+oBq6lH5O8BxqMP+zH15AshUR0P4
si/LMG8cNXKPgfs6C3qkT+fQEhWkP/HP/roCYIXPRtDqBmD0qlThGWVetlp8ziEW
8i8XnfZFIQF9shKI5aV0CymRAgMBAAGjZjBkMB0GA1UdDgQWBBRyndsZlRIKg3eY
DWTFEbrCWnCibTAfBgNVHREEGDAWgQ5lbWFpbEBhY21lLmNvbYcEfwAAATAOBgNV
HQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG9w0BAQsFAAOC
AQEARuFq0mW8Wcru7azu5DNGyuCL43jnnGKRcCTlGzZkoJFIebOAowufoZhlvCHV
yHTlJdEbhRMth6Opnwd82ub/qHtB/hwXwXUG0p/9N+qS52yogFJvlmansdno/gfD
w0zSO84tCRv5M3N4IT6i5TS0/kFNx8PY38wLEXo9+DXai/64weiT2T5n6s/cQMgg
IFYslUkRiGyfDLVHztIboCTNYjHBAjlusp49QBNnK4Grh1tFdB5S3hosvcm9Adkh
XmiC+WSkUNtJIGiW/4etupAF8f2cOmqq61KCxOCFWHMuu4lfgosKumxqKUYKmePn
Bqv5ED0zw+dXSSateew1atlwDw==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEFTCCAv2gAwIBAgIJANQKp+hGlaGuMA0GCSqGSIb3DQEBCwUAMIGVMQswCQYD
```

```
    VQQDDAJDQTEXMBUGCgmSJomT8ixkARkWB3ZzcGhlcmUxFTATBgoJkiaJk/IsZAEZ
    FgVsb2NhbDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFzAVBgNV
    BAoMDnBob3Rvbi1tYWNoaW5lMRswGQYDVQQLDBJWTXdhcmUgRW5naW5lZXJpbmcw
    HhcNMjEwOTI1MTE1MTI2WhcNMzEwOTIzMTE1MTI2WjCBlTELMAkGA1UEAwwCQ0Ex
    FzAVBgoJkiaJk/IsZAEZFgd2c3BoZXJlMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwx
    CzAJBgNVBAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRcwFQYDVQQKDA5waG90
    b24tbWFjaGluZTEbMBkGA1UECwwSVk13YXJlIEVuZ2luZWVyaW5nMIIBIjANBgkq
    hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAunLr3P9x/6SL/hee5cCsOEsDVkqn+5wX
    T1Qq+hAyFY909ARGXtmxQfczzBg322XUHRr/hCOzzKPBdurclXRjCf8t8h4N2Xij
    UoO1sc4j0jQspLfIi8bvbzwIZ1JRRWVAXT0SkjyS7LxG6OqY3S3jt5uHZIvn9ivN
    jACsZ6jOrJvr6yHXGVBhnzGvQMfbwM/fMoQw6lzBRLpO1+9YvYNzAxmeu70jh9l+
    Cj5xF2lH9t0dxADpeOiayHYox5hpAX9kRL+QnyyImEUTLUk36DCwL96h7+UnK4ca
    xrxUFuWp/BU/OJTaIGJze5IiF9XlDkSw3sgvDmKGdYhWsv9UvxtgJQIDAQABo2Yw
    ZDAdBgNVHQ4EFgQUERbyxK4Rwmuc9ETdx2sbcgyG/uowHwYDVR0RBBgwFoEOZW1h
    aWxAYWNtZS5jb22HBH8AAAEwDgYDVR0PAQH/BAQDAgEGMBIGA1UdEwEB/wQIMAYB
    Af8CAQAwDQYJKoZIhvcNAQELBQADggEBAFej6jp93JPmkd/AIoLBItv55LIBlTpF
    32JExgFOLXhZUl3v/wUXg13yPFbL3B8MK0bxADaXhIjsiF7fbGBLnQ0jBbDnLxCE
    LLTxww9c0EOxsQJPe/E9GlJm1WEogT5c+VyggZUhZ/AEOwOZJ+99V+pHapRoh/8S
    EzCxv4rH025/iHujNSQYS69FcGoh/kq0OfVPiFkeWYqzUctXClU4GPp+PLE4N+Ky
    pxIN6g7IHujIIq+8q6Xg6JXKJMrAvnR3X0fNUWD8knAESnTweC1tRSH3zJ08Pi9V
    13MAhubAeOOXEfQ04v/hh+a/AoaSnt0A0YawKpefG4w4rwz6XzJ80lg=
    -----END CERTIFICATE-----
    -----BEGIN CERTIFICATE-----
    MIIEODCCAyCgAwIBAgIJAN2uLgGrABJwMA0GCSqGSIb3DQEBCwUAMIG3MSQwIgYD
    VQQDDBtSWi1DQUdTLVZDU0EwMDEuQ0FSSVBSUEMuSVQxFzAVBgoJkiaJk/IsZAEZ
    Fgd2c3BoZXJlMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxCzAJBgNVBAYTAklUMQ8w
    DQYDVQQIDAZNaWxhbm8xJDAiBgNVBAoMG1JaLUNBR1MtVkNTQTAwMS5jYXJpcHJw
    Yy5pdDEbMBkGA1UECwwSVk13YXJlIEVuZ2luZWVyaW5nMB4XDTIzMTAxODA4NTUx
    MFoXDTMzMTAxNTA4NTUxMFowgbcxJDAiBgNVBAMMG1JaLUNBR1MtVkNTQTAwMS5D
    QVJJUFJQQy5JVDEXMBUGCgmSJomT8ixkARkWB3ZzcGhlcmUxFTATBgoJkiaJk/Is
    ZAEZFgVsb2NhbDELMAkGA1UEBhMCSVQxDzANBgNVBAgMBk1pbGFubzEkMCIGA1UE
    CgwbUlotQ0FHUy1WQ1NBMDAxLmNhcmlwcnBjLml0MRswGQYDVQQLDBJWTXdhcmUg
    RW5naW5lZXJpbmcwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCpEHua
    mGn3Q4Z3ZRWloSlWXjhRNQoijWDdOnJIO8xHBhmVXycmSELfZTzaTK/yocBtWDHR
    Yf60BHmcX3+mTV57eYUzjWPj0pTsgTX+eBVyRjso3RlvYDzfg2QqlLxbMFvN8j7v
    y7qxhXGnhVypwadBdMkw5VGCo5EKfzA3m6xC9Od9dnvvvPNpWGUdndjYuZM2eRNj
    Mng01Pbn6c961nkwLmhDtz+wuu26iNvAwx6YT0n9oJaiBAps9+Ke8+tJ2Fue6fVU
    frLtWWvTa+C0MdJ71QBgGdCtxmBqcITtuOumqD3LjZUo8CDOUHRD3aXKAOcbkqV3
    qF36yn3QK0OqHeZvAgMBAAGjRTBDMB0GA1UdDgQWBBRWdiHX/T+REpd0RAArMdCC
    nqzuHDAOBgNVHQ8BAf8EBAMCAQYwEgYDVR0TAQH/BAgwBgEB/wIBADANBgkqhkiG
    9w0BAQsFAAOCAQEAWZxSTt9EiAt+6rHADSWgg2vZ9mxYT4ttihhKN2iDJJO5X3ii
    eUo5uEjY1eF6SqCwTyQB6MOWTdEg/y7Wk+2MJrzRXz0WnlUrSz/tbkfH5PFlrft+
    UivDuoHVKpy9n6wxSU7iC0LqPLonyOm289XEmglTs4H2268UoV49Rt2P9CSLjwan
    xIRUVnLocoN1VeknO5sXVnIN79upwgkl1gAPs1ZnEBwDVkZYRtEJipjvayc9TzFc
    6U0om4oIYcbQI5ZFr/VzUfKAatTGiY2Bj1HoNL3yidUDwrZXmZABuY6aG8hJ6Iqu
    p/yrguErGymmq5RmvxrM/U5iFgVY/eixvTT3BA==
    -----END CERTIFICATE-----

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat secret-creds.yaml
apiVersion: v1
stringData:
  password: 'XXXXXXXXX'
  username: "cariprpc\\cp_12_vcenter_OCP"
kind: Secret
metadata:
  name: ocp1-parallelo-vsphere-creds
  namespace: ocp1-parallelo
```

```
type: Opaque

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat clusterdeployment.yaml
apiVersion: hive.openshift.io/v1
kind: ClusterDeployment
metadata:
  labels:
    cloud: vSphere
    vendor: OpenShift
  name: ocp1-parallelo
  namespace: ocp1-parallelo
spec:
  baseDomain: cariprpcpar.it
  clusterName: ocp1-parallelo
  controlPlaneConfig:
    servingCertificates: {}
  installAttemptsLimit: 1
  installed: false
  platform:
    vsphere:
      certificatesSecretRef:
        name: ocp1-parallelo-vsphere-certs
      cluster: OCP_PREPROD
      credentialsSecretRef:
        name: ocp1-parallelo-vsphere-creds
      datacenter: ACILIA
      defaultDatastore: ESX-OCP-PREPROD-AC-0000
      folder: /ACILIA/vm/PARALLELO/OCP
      network: dvpg_620_DMZ_ocprhel_par
      vCenter: ac-cags-vcsa001.cariprpc.it
  provisioning:
    imageSetRef:
      name: img4.14.2-x86-64
    installConfigSecretRef:
      name: ocp1-parallelo-install-config
    sshPrivateKeySecretRef:
      name: ocp1-parallelo-ssh-private-key
  pullSecretRef:
    name: ocp1-parallelo-pull-secret

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat machinepool-infra.yaml
apiVersion: hive.openshift.io/v1
kind: MachinePool
metadata:
  name: ocp1-parallelo-infra
  namespace: ocp1-parallelo
spec:
  clusterDeploymentRef:
    name: ocp1-parallelo
  name: infra
  platform:
    vsphere:
      coresPerSocket: 2
      cpus: 16
      memoryMB: 32768
      osDisk:
        diskSizeGB: 120
  replicas: 0
[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat machinepool-odf.yaml
apiVersion: hive.openshift.io/v1
kind: MachinePool
metadata:
  name: ocp1-parallelo-odf
  namespace: ocp1-parallelo
spec:
  clusterDeploymentRef:
    name: ocp1-parallelo
  name: odf
  platform:
    vsphere:
      coresPerSocket: 2
      cpus: 16
      memoryMB: 32768
      osDisk:
        diskSizeGB: 120
  replicas: 0

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat managedcluster.yaml
apiVersion: cluster.open-cluster-management.io/v1
kind: ManagedCluster
metadata:
  labels:
    cloud: vSphere
    name: 'ocp1-parallelo'
    vendor: OpenShift
  name: 'ocp1-parallelo'
spec:
  hubAcceptsClient: true

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat install-config.yaml
apiVersion: v1
metadata:
  name: ocp1-parallelo
baseDomain: cariprpcpar.it
proxy:
  httpProxy: http://vip-navproxy-server.cariprpc.it:8080
  httpsProxy: http://vip-navproxy-server.cariprpc.it:8080
  noProxy:
localhost,127.0.0.1,localaddress,.localdomain.com,.cariprpcpar.it,172.30.0.0/16,169.254.0.0/16,.cariprpc.it,10.215.87.0/24
controlPlane:
  name: master
  hyperthreading: Enabled
  replicas: 3
  platform:
    vsphere:
      cpus: 16
      coresPerSocket: 2
      memoryMB: 32768
      osDisk:
        diskSizeGB: 120
compute:
  - name: worker
    hyperthreading: Enabled
    replicas: 3
    platform:
      vsphere:
        cpus: 16
        coresPerSocket: 2
        memoryMB: 32768
        osDisk:
          diskSizeGB: 120
networking:
  networkType: OVNKubernetes
  clusterNetwork:
    - cidr: 10.128.0.0/14
      hostPrefix: 23
  machineNetwork:
    - cidr: 10.215.87.0/24
  serviceNetwork:
    - 172.30.0.0/16
platform:
  vsphere:
    vCenter: ac-cags-vcsa001.cariprpc.it
    username: cariprpc\cp_12_vcenter_OCP
    password: XXXXXXXXXXXXXXXXXXX
    datacenter: ACILIA
    defaultDatastore: ESX-OCP-PREPROD-AC-0000
    cluster: OCP_PREPROD
    apiVIP: 10.215.87.14
    ingressVIP: 10.215.87.13
    network: dvpg_620_DMZ_ocprhel_par
    folder: /ACILIA/vm/PARALLELO/OCP
pullSecret: ''
sshKey: ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAINXQWDylUR5IzHTI0R2eWkRHqZeIfIo7X+qjxoBrRAwW
root@grpi-ocp-hv00

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat pull-secret.txt
{"auths":{"cloud.openshift.com":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc3
NfZTdjYzcwZDhkNjZlNGE1MTgxYWZlOTAzYTNiMTI2NDk6TjZHSFpKUTI4RFExNEgzT05PVlQ2UTZYUU4zM
U40UU9TVzRYTFNEVjdUOElBVDA3V01VTFpVSFBFQzRYTkFSVg==","email":"daniele.bagiotti@cred
it-agricole.it"},"quay.io":{"auth":"b3BlbnNoaWZ0LXJlbGVhc2UtZGV2K29jbV9hY2Nlc3NfZTd
jYzcwZDhkNjZlNGE1MTgxYWZlOTAzYTNiMTI2NDk6TjZHSFpKUTI4RFExNEgzT05PVlQ2UTZYUU4zMU40UU
9TVzRYTFNEVjdUOElBVDA3V01VTFpVSFBFQzRYTkFSVg==","email":"daniele.bagiotti@credit-ag
ricole.it"},"registry.connect.redhat.com":{"auth":"fHVoYy1wb29sLTgxNGFiODI0LTgwMzct
NGJjMy1iMTA2LWUwZDQyMWY5NDU2ZjpleUpoYkdjaU9pSlNVelV4TWlKOS5leUp6ZFdJaU9pSTJNekZpWW1
Ka09XTXlOVGswWTJaak9UWm1abUkwWVRRMU4yTmhORE00TVNKOS5jdVU0TjA4R3Q5VUh6Snk0d3VXOV9aeF
dTc1FiN0dUYThWRm0yTTdqWFBmSXd3TXZ0YnZGTHVwYno5bTZZX3VXTE91UF9SZk9xSVpldGk1X3oxUnBNO
FVnRDMzUUJ2V2QxbGFxMkJEY0ZUTHlyQ2Z5anVvaGdvZFppZE5SRFgwQXRURFdDLTlOMmRlMTZMUWhaeUtt
YnBaZlFDVVo5TGtDLWdQSk1xVmNTOFY3RzhXM2x0QWkyTm55TGp1dzBDMk5MUjl3M3R4M29tRnhES1Jabm1
kYmFQemdzQ2o4bnNCZXhDYmtYRFVCVWo1YUFjX1Fha3FxNVZZYmtxYTQtNHRZYTljamc3RXEtUy11dW5pWl
o3cldxLUhOdmlYRUpWVVY0M1NkdnlNZ2I0bTQwanFaYVpqOVpLQ1pycktVUdnd0tTS1IteUNwcHhWZWZSc
nB0QmZ4WndrM0ZPNGg1azZuOUdOSE1RazdmRGVnTEJ5WVdmcVdQNnZHSENudW1LRVFBLWczcXBPZENrWlpt
V2VRQlpHaExxHNkhpS0luRHVIOUxKb2hhSm5BcTBqVVhsVHdGYWZ4OUtoVXhUemM1cDhBUmQwZGdEd2tUZjJ
aVWZKM2czVW1QUjNHaTRmY2xTaHc5RW9UbXlKXzYzdHpSV0pJd053X0VSOE9QSHVnNFNwM2pfZ2lPaXNCSm
I2TU5ybkJ3WmFXWElDNjdCbnR2REJVTXgyZkdYbDJ2cDZEamdpWjZxU2Z5blRwWXFpaFBGSWplbldQd0VqU
Fl5b01nQTF2NVJoanppT1ZCemZXRTVKY1pOdC1VaU5GckdaMmV0bXdQUkpNaThJODJ2YWx3SjlxYkNZT21f
Q2xsRWI4TEF0aWJDTGtyYUVPRmY2cmpyMGRSUXZ1VlRIb3BJTQ==","email":"daniele.bagiotti@cre
dit-agricole.it"},"registry.redhat.io":{"auth":"fHVoYy1wb29sLTgxNGFiODI0LTgwMzctNGJ
jMy1iMTA2LWUwZDQyMWY5NDU2ZjpleUpoYkdjaU9pSlNVelV4TWlKOS5leUp6ZFdJaU9pSTJNekZpWW1Ka0
9XTXlOVGswWTJaak9UWm1abUkwWVRRMU4yTmhORE00TVNKOS5jdVU0TjA4R3Q5VUh6Snk0d3VXOV9aeFdTc
1FiN0dUYThWRm0yTTdqWFBmSXd3TXZ0YnZGTHVwYno5bTZZX3VXTE91UF9SZk9xSVpldGk1X3oxUnBNOFVn
RDMzUUJ2V2QxbGFxMkJEY0ZUTHlyQ2Z5anVvaGdvZFppZE5SRFgwQXRURFdDLTlOMmRlMTZMUWhaeUttYnB
aZlFDVVo5TGtDLWdQSk1xVmNTOFY3RzhXM2x0QWkyTm55TGp1dzBDMk5MUjl3M3R4M29tRnhES1Jabm1kYm
FQemdzQ2o4bnNCZXhDYmtYRFVCVWo1YUFjX1Fha3FxNVZZYmtxYTQtNHRZYTljamc3RXEtUy11dW5pWlo3c
ldxLUhOdmlYRUpWVVY0M1NkdnlNZ2I0bTQwanFaYVpqOVpLQ1pycktKVUdnd0tTS1IteUNwcHhWZWZScnB0
QmZ4WndrM0ZPNGg1azZuOUdOSE1RazdmRGVnTEJ5WVdmcVdQNnZHSENudW1LRVFBLWczcXBPZENrWlptV2V
RQlpHaExHNkhpS0luRHVIOUxKb2hhSm5BcTBqVVhsVHdGYWZ4OUtoVXhUemM1cDhBUmQwZGdEd2tUZjJaVW
ZKM2czVW1QUjNHaTRmY2xTaHc5RW9UbXlKXzYzdHpSV0pJd053X0VSOE9QSHVnNFNwM2pfZ2lPaXNCSmI2T
U5ybkJ3WmFXWElDNjdCbnR2REJVTXgyZkdYbDJ2cDZEamdpWjZxU2Z5blRwWXFpaFBGSWplbldQd0VqUFl5
b01nQTF2NVJoanppT1ZCemZXRTVKY1pOdC1VaU5GckdaMmV0bXdQUkpNaThJODJ2YWx3SjlxYkNZT21fQ2x
sRWI4TEF0aWJDTGtyYUVPRmY2cmpyMGRSUXZ1VlRIb3BJTQ==","email":"daniele.bagiotti@credit
-agricole.it"}}}

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat ssh-pub-key.txt
ssh-ed25519    AAAAC3NzaC1lZDI1NTE5AAAAINXQWDylUR5IzHTI0R2eWkRHqZeIfIo7X+qjxoBrRAwW
root@grpi-ocp-hv00

[root@grpi-ocp-hv00 ocp1-parallelo-template]# cat ssh-key.txt
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAAAMwAAAAtzc2gtZW
QyNTUxOQAAACDV0Fg8pVEeSMx0yNEdnlpER6mXiHyKO1/qo8aAa0QMFgAAAJhlVFRFZVRU
RQAAAAtzc2gtZWQyNTUxOQAAACDV0Fg8pVEeSMx0yNEdnlpER6mXiHyKO1/qo8aAa0QMFg
AAAEATfIEZKZ+IqyLLX4nv2QDbagivPwzhm5PTh8SJO//Z/dXQWDylUR5IzHTI0R2eWkRH
qZeIfIo7X+qjxoBrRAwWAAAAEnJvb3RAZ3JwaS1vY3AtaHYwMAECAw==
-----END OPENSSH PRIVATE KEY-----
```

I cluster è stato installato utilizzando il seguente comando:

```
Python
[root@grpi-ocp-hv00 ~]# cd /root/ocp-acm/deploy-cluster
[root@grpi-ocp-hv00 deploy-cluster]# oc apply -k ./ocp1-parallelo-template/
```

Una volta terminati i task di creazione del cluster sarà possibile visualizzarne l’fqdn delle API e le credenziali per l’autenticazione accedendo alla dashboard ACM e selezionando Infrastruttura/Cluster.

IMPORTANTE: il template secret-certs.yaml contiene tutti i certificati del vCenter la quale estensione termina con “.0”.

All’interno della directory “**/root/ocp-acm/policy-generator/ocp1-parallelo**” sono state create le policy per il cluster ocp1-parallelo, nei prossimi paragrafi verranno descritte puntualmente.

3.2. Configurazioni aggiuntive

3.2.1. Nodi worker

Per questioni di capacity lato piattaforma sottostante, è stato necessario definire un pool di nodi worker che utilizzassero un datastore differente da quello di default.

Per far questo sono stati svolti i seguenti step:

1. Scale a 0 del MachinePool dei worker
2. Eliminazione del machineset dei worker
3. Creazione nuovo machineset con puntamento al datastore non di default tramite policy ACM

Per scalare il MachinePool dei worker collegarsi alla console di ACM e all'interno dei dettagli del cluster, cliccare sul tab MachinePool, andare in edit sulla replica del machinePool dei worker portandola a 0.

Per eliminare il machineset dei worker con il datastore di default, eseguire i seguenti comandi:

```
Python
[root@grpi-ocp-hv00 ~]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 ~]# oc delete machineset ocp1-parallelo-6ldrf-worker-0
```

All'interno della directory worker-nodes sono stati creati template per creare il *machineset* dei nuovi nodi worker:

```
Python
[root@grpi-ocp-hv00 worker-nodes]# ll
/root/ocp-acm/policy-generator/ocp1-parallelo/worker-nodes
-rw-r--r--. kustomization.yaml
-rw-r--r--. machine-set-worker.yaml
-rw-r--r--. worker-nodes-conf.yaml


[root@grpi-ocp-hv00 worker-nodes]# cat kustomization.yaml
```

```
generators:
  - worker-nodes-conf.yaml

[root@grpi-ocp-hv00 worker-nodes]# cat worker-nodes-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-worker-node-conf-ocp1
placementBindingDefaults:
  name: placement-binding-worker-node-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-worker-node-ms-ocp1
    manifests:
      - path: machine-set-worker.yaml

[root@grpi-ocp-hv00 worker-nodes]# cat machine-set-worker.yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: ocp1-parallelo-6ldrf-worker-0
  namespace: openshift-machine-api
spec:
  selector:
    matchLabels:
      machine.openshift.io/cluster-api-cluster: ocp1-parallelo-6ldrf
      machine.openshift.io/cluster-api-machineset: ocp1-parallelo-6ldrf-worker-0
  template:
    metadata:
      labels:
        machine.openshift.io/cluster-api-cluster: ocp1-parallelo-6ldrf
        machine.openshift.io/cluster-api-machine-role: worker
        machine.openshift.io/cluster-api-machine-type: worker
        machine.openshift.io/cluster-api-machineset: ocp1-parallelo-6ldrf-worker-0
    spec:
      lifecycleHooks: {}
      metadata: {}
      providerSpec:
        value:
          apiVersion: machine.openshift.io/v1beta1
          credentialsSecret:
            name: vsphere-cloud-credentials
          diskGiB: 120
          kind: VSphereMachineProviderSpec
          memoryMiB: 32768
          metadata:
            creationTimestamp: null
          network:
            devices:
            - networkName: dvpg_620_DMZ_ocprhel_par
          numCPUs: 16
          numCoresPerSocket: 2
          snapshot: ""
          template: ocp1-parallelo-6ldrf-rhcos-generated-region-generated-zone
          userDataSecret:
            name: worker-user-data
          workspace:
            datacenter: ACILIA
            datastore: /ACILIA/datastore/ESX-OCP-PREPROD-AC-0001
            folder: /ACILIA/vm/PARALLELO/OCP
            resourcePool: /ACILIA/host/OCP_PREPROD//Resources
            server: ac-cags-vcsa001.cariprpc.it
```

Per creare la policy associata, è stato eseguito il seguente comando:

Python

```
[root@grpi-ocp-hv00 worker-nodes]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 worker-nodes]# oc kustomize --enable-alpha-plugins=true . | oc
apply -f
```

Al termine della creazione, modificare la replica del *machineset* dei worker come segue:

Python

```
[root@grpi-ocp-hv00 worker-nodes]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 worker-nodes]# oc scale --replicas=6 machineset
ocp1-parallelo-6ldrf-worker-0
```

3.2.2. Servizio Chronyd

All'interno della directory **ntp-conf** sono stati definiti i template necessari a configurare il servizio *chronyd* sulle macchine virtuali di OCP.

Python

```
[root@grpi-ocp-hv00 acm-hub]# ll
/root/ocp-acm/policy-generator/ocp1-parallelo/ntp-conf
-rw-r--r--. kustomization.yaml
-rw-r--r--. ntp-conf.yaml
-rw-r--r--. ntp-master-conf.yaml
-rw-r--r--. ntp-worker-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat kustomization.yaml
generators:
  - ntp-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-ntp-conf-ocp
placementBindingDefaults:
  name: placement-binding-ntp-conf-ocp
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: local-cluster
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-ntp-master-ocp
    manifests:
      - path: ntp-master-conf.yaml
  - name: policy-ntp-worker-ocp
    manifests:
      - path: ntp-worker-conf.yaml

[root@grpi-ocp-hv00 ntp-conf]# cat ntp-master-conf.yaml
# Generated by Butane; do not edit
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: master
  name: 99-master-custom-ntp
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            compression: gzip
                                                                             source:
data:;base64,H4sIAAAAAAAC/2TLwQ3DIAyF4bun8AQGQi8dJyEOQaUYGTdStq9a5Zbb0/v1dZGKnnTnSr
9NzTqJZizLR4fBYD1YMXiaQqTwoOCf9zNOsGrZbCuV0R2zuloWl3aVdrp/gff84mHcMZDHCGppnC1BlbwWv
Yzky8A3AAD//9ME84KXAAAA
          mode: 420
          overwrite: true
          path: /etc/chrony.conf
```

```
[root@grpi-ocp-hv00 ntp-conf]# cat ntp-worker-conf.yaml
# Generated by Butane; do not edit
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-worker-custom-ntp
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            compression: gzip
                                                                             source:
data:;base64,H4sIAAAAAAAC/2TLwQ3DIAyF4bun8AQGQi8dJyEOQaUYGTdStq9a5Zbb0/v1dZGKnnTnSr
9NzTqJZizLR4fBYD1YMXiaQqTwoOCf9zNOsGrZbCuV0R2zuloWl3aVdrp/gff84mHcMZDHCGppnC1BlbwWv
Yzky8A3AAD//9ME84KXAAAA
          mode: 420
          overwrite: true
          path: /etc/chrony.conf
```

I file **ntp-master-conf.yaml** e **ntp-worker-conf.yaml** sono stati copiati da quelli utilizzati dal cluster ACM perchè gli NTP utilizzati sono gli stessi.

A questo punto sono state create le policy con il comando seguente:

```
Python
[root@grpi-ocp-hv00 ntp-conf]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 ntp-conf]# oc kustomize --enable-alpha-plugin=true . | oc apply
-f -
```

IMPORTANTE: la configurazione del servizio *chronyd* prevede il riavvio di tutti i nodi del cluster in maniera *rolling*. Attendere che tutti i nodi vengano riavviati prima di passare allo step successivo.

3.2.3. Definizione nodi infrastrutturali

All'interno della directory **infra-nodes** sono stati definiti i template necessari a:

- Creare il *machineconfigpool* per i nodi infrastrutturali

- Aggiungere taint e label ai nodi infrastrutturali

Python

```
[root@grpi-ocp-hv00 infra-nodes]# ll
/root/ocp-acm/policy-generator/ocp1-parallelo/infra-nodes
-rw-r--r--. taint-infra.yaml
-rw-r--r--. infra-nodes-conf.yaml
-rw-r--r--. kustomization.yaml
-rw-r--r--. mcp-infra.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat kustomization.yaml
generators:
  - infra-nodes-conf.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat infra-nodes-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-infra-node-conf-ocp1
placementBindingDefaults:
  name: placement-binding-infra-node-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-infra-node-taint-ocp1
    manifests:
      - path: taint-infra.yaml
  - name: policy-infra-node-mcp-ocp1
    manifests:
      - path: mcp-infra.yaml

[root@grpi-ocp-hv00 infra-nodes]# cat taint-infra.yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: ocp1-parallelo-6ldrf-infra-0
  namespace: openshift-machine-api
spec:
  template:
    spec:
      metadata:
        labels:
          node-role.kubernetes.io/infra: ""
      taints:
      - key: node-role.kubernetes.io/infra
        effect: NoSchedule

[root@grpi-ocp-hv00 infra-nodes]# cat mcp-infra.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
```

```
metadata:
  name: infra
spec:
  machineConfigSelector:
    matchExpressions:
    - key: machineconfiguration.openshift.io/role
      operator: In
      values:
      - worker
      - infra
  nodeSelector:
    matchExpressions:
    - key: node-role.kubernetes.io/infra
      operator: Exists
    - key: cluster.ocs.openshift.io/openshift-storage
      operator: DoesNotExist
```

Per creare le policy è stato eseguito il seguente comando:

```
Python
[root@grpi-ocp-hv00 infra-nodes]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 infra-nodes]# oc kustomize --enable-alpha-plugin=true . | oc
apply -f -
```

A questo punto portare a 3 la replica del MachinePool dei nodi infra tramite dashboard ACM, verificare che sul cluster ocp1-parallelo i nodi infrastrutturali siano 3 e che il *machineconfigpool* contenga correttamente i nodi infra.

3.2.4. Definizione nodi storage

All’interno della directory **odf-nodes** sono stati definiti i template necessari a:

- Creare il *machineconfigpool* per i nodi storage
- Aggiungere taint e label ai nodi infrastrutturali

```
Python
[root@grpi-ocp-hv00 odf-nodes]# ll
/root/ocp-acm/policy-generator/ocp1-parallelo/odf-nodes
-rw-r--r--. taint-odf.yaml
-rw-r--r--. odf-nodes-conf.yaml
-rw-r--r--. kustomization.yaml
```

```
-rw-r--r--. mcp-odf.yaml

[root@grpi-ocp-hv00 odf-nodes]# cat kustomization.yaml
generators:
  - odf-nodes-conf.yaml

[root@grpi-ocp-hv00 odf-nodes]# cat odf-nodes-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-odf-node-conf-ocp1
placementBindingDefaults:
  name: placement-binding-odf-node-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-odf-node-taint-ocp1
    manifests:
      - path: taint-odf.yaml
  - name: policy-odf-node-mcp-ocp1
    manifests:
      - path: mcp-odf.yaml

[root@grpi-ocp-hv00 odf-nodes]# cat mcp-odf.yaml
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfigPool
metadata:
  name: storage
spec:
  machineConfigSelector:
    matchExpressions:
    - key: machineconfiguration.openshift.io/role
      operator: In
      values:
      - worker
      - infra
  nodeSelector:
    matchExpressions:
    - key: cluster.ocs.openshift.io/openshift-storage
      operator: Exists

[root@grpi-ocp-hv00 odf-nodes]# cat taint-odf.yaml
apiVersion: machine.openshift.io/v1beta1
kind: MachineSet
metadata:
  name: ocp1-parallelo-6ldrf-odf-0
  namespace: openshift-machine-api
spec:
  template:
    spec:
      metadata:
```

```
    labels:
     node-role.kubernetes.io/infra: ""
     cluster.ocs.openshift.io/openshift-storage: ""
   taints:
   - effect: NoSchedule
    key: node.ocs.openshift.io/storage
    value: "true"
```

Per creare le policy è stato eseguito il seguente comando:

```
Python
[root@grpi-ocp-hv00 odf-nodes]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 odf-nodes]# oc kustomize --enable-alpha-plugin=true . | oc
apply -f -
```

A questo punto portare a 3 la replica del MachinePool dei nodi storage tramite dashboard ACM, verificare che sul cluster ocp1-parallelo i nodi storage siano 3 e che il machineconfigpool contenga correttamente i nodi odf.

3.2.4.1. Aggiunta dischi per ODF

Visto che questi tre nodi devono ospitare la componente ODF, è necessario aggiungere a queste 3 macchine virtuali un disco da 1TB.

Questa operazione è stata eseguita manualmente collegandosi alla dashboard del vCenter.

3.2.5. Installazione ODF

Vista l'importanza di allineare le versioni dell'operator dello storage tra collaudo e parallelo, e l'importanza dell'operator dello storage, si è optato per non utilizzare l'approccio delle policy ma di templetizzare l'installazione così da poter utilizzare gli stessi template sia sul cluster di Acilia che su quello di Rozzano.

Per far questo all'interno della directory **/root/ocp-acm/cluster-template** è stata creata la directory **odf-installation**, suddivisa a sua volta in due directory che contengono i template dei due due operator necessari ad eseguire il deploy della componente storage: **local-storage** e **openshift-storage**.

3.2.5.1. Local storage operator

Riporto i template della componente local-storage:

Python

```
[root@grpi-ocp-hv00 local-storage]# ll
-rw-r--r--. kustomization.yaml
-rw-r--r--. namespace.yaml
-rw-r--r--. operatorgroup.yaml
-rw-r--r--. subscription.yaml
-rw-r--r--. localvolumediscovery.yaml
-rw-r--r--. localvolumeset.yaml
-rw-r--r--. GENERIClocalvolumeset.yaml

[root@grpi-ocp-hv00 local-storage]# cat kustomization.yaml
resources:
- namespace.yaml
- operatorgroup.yaml
- subscription.yaml
generatorOptions:
  disableNameSuffixHash: true

[root@grpi-ocp-hv00 local-storage]# cat namespace.yaml
apiVersion: v1
kind: Namespace
metadata:
   name: openshift-local-storage
   spec: {}

[root@grpi-ocp-hv00 local-storage]# cat operatorgroup.yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
 name: local-operator-group
 namespace: openshift-local-storage
spec:
 targetNamespaces:
 - openshift-local-storage

[root@grpi-ocp-hv00 local-storage]# cat subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: local-storage-operator
  namespace: openshift-local-storage
spec:
  channel: stable
  installPlanApproval: Manual
  name: local-storage-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
  startingCSV: local-storage-operator.v4.14.0-202402221640
```

Per installare l'operator del **local-storage** sono stati eseguiti i seguenti comandi:

Python

```
[root@grpi-ocp-hv00 local-storage]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it
[root@grpi-ocp-hv00 local-storage]# oc apply -k .
```

A questo punto è necessario collegarsi alla dashboard dell'ambiente ocp1-parallelo ed eseguire manualmente l'approvazione dell'installation plan.

Terminata questa fase è possibile creare il *localvolumeset* e il meccanismo di discovery dei dischi tramite i seguenti comandi:

Python

```
[root@grpi-ocp-hv00 local-storage]# cat localvolumeset.yaml
apiVersion: local.storage.openshift.io/v1alpha1
kind: LocalVolumeSet
metadata:
  name: local-volume-set
  namespace: openshift-local-storage
spec:
  deviceInclusionSpec:
    deviceTypes:
    - disk
    - part
    minSize: 150Gi
  nodeSelector:
    nodeSelectorTerms:
    - matchExpressions:
      - key: kubernetes.io/hostname
        operator: In
        values:
        - ocp1-parallelo-6ldrf-odf-0-5ptzd
        - ocp1-parallelo-6ldrf-odf-0-9kf59
        - ocp1-parallelo-6ldrf-odf-0-q76tw
  storageClassName: local-volume-set
  tolerations:
  - effect: NoSchedule
    key: node.ocs.openshift.io/storage
    operator: Equal
    value: "true"
  volumeMode: Block
[root@grpi-ocp-hv00 local-storage]# cat localvolumediscovery.yaml
apiVersion: local.storage.openshift.io/v1alpha1
kind: LocalVolumeDiscovery
metadata:
 name: auto-discover-devices
 namespace: openshift-local-storage
spec:
 nodeSelector:
   nodeSelectorTerms:
     - matchExpressions:
       - key: cluster.ocs.openshift.io/openshift-storage
         operator: In
         values:
           - ""


[root@grpi-ocp-hv00 local-storage]# oc create -f localvolumeset.yaml
[root@grpi-ocp-hv00 local-storage]# oc create -f localvolumediscovery.yaml
```

A questo punto è possibile verificare la creazione dei volumi sui dischi aggiuntivi da 1 TB con il comando:

```
Python
[root@grpi-ocp-hv00 local-storage]# oc project openshift-local-storage
[root@grpi-ocp-hv00 local-storage]# oc get pvc
```

3.2.5.2. Openshift Storage operator

Seguono i template creati per installare e configurare l’operator di Openshift Data Foundation:

```
Python
[root@grpi-ocp-hv00 openshift-storage]# ll
-rw-r--r--. namespace.yaml
-rw-r--r--. operatorgroup.yaml
-rw-r--r--. subscription.yaml
-rw-r--r--. console-plugin.yaml
-rw-r--r--. ocs-storage-cluster.yaml
-rw-r--r--. rook-ceph-operator-config.yaml
-rw-r--r--. OCSInitialization.yaml

[root@grpi-ocp-hv00 openshift-storage]# cat namespace.yaml
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  name: openshift-storage
spec:
 {}

[root@grpi-ocp-hv00 openshift-storage]# cat operatorgroup.yaml
```

```
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-storage
  namespace: openshift-storage
spec:
  targetNamespaces:
  - openshift-storage

[root@grpi-ocp-hv00 openshift-storage]# cat subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: odf-operator
  namespace: openshift-storage
spec:
  channel: stable-4.14
  installPlanApproval: Manual
  name: odf-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
  startingCSV: odf-operator.v4.14.5-rhodf

[root@grpi-ocp-hv00 openshift-storage]# cat console-plugin.yaml
apiVersion: operator.openshift.io/v1
kind: Console
metadata:
  name: cluster
spec:
  logLevel: Normal
  managementState: Managed
  operatorLogLevel: Normal
  plugins:
  - logging-view-plugin
  - monitoring-plugin
  - odf-console

[root@grpi-ocp-hv00 openshift-storage]# cat ocs-storage-cluster.yaml
apiVersion: ocs.openshift.io/v1
kind: StorageCluster
metadata:
  name: ocs-storagecluster
  namespace: openshift-storage
spec:
  arbiter: {}
  encryption:
    kms: {}
  externalStorage: {}
  flexibleScaling: true
  managedResources:
    cephBlockPools: {}
    cephCluster: {}
    cephConfig: {}
    cephDashboard: {}
    cephFilesystems: {}
    cephNonResilientPools: {}
    cephObjectStoreUsers: {}
    cephObjectStores: {}
    cephRBDMirror: {}
    cephToolbox: {}
  mirroring: {}
  monDataDirHostPath: /var/lib/rook
  network:
    connections:
      encryption: {}
    multiClusterService: {}
  nodeTopologies: {}
  storageDeviceSets:
  - config: {}
    count: 3
    dataPVCTemplate:
      metadata: {}
      spec:
        accessModes:
        - ReadWriteOnce
        resources:
          requests:
            storage: "1"
        storageClassName: local-volume-set
        volumeMode: Block
    name: ocs-deviceset-local-volume-set
    placement: {}
    preparePlacement: {}
    replica: 1
    resources: {}
[root@grpi-ocp-hv00 openshift-storage]# cat rook-ceph-operator-config.yaml
apiVersion: v1
data:
  CSI_ENABLE_CSIADDONS: "true"
  CSI_LOG_LEVEL: "5"
  CSI_PLUGIN_TOLERATIONS: |-
    - key: node.ocs.openshift.io/storage
      operator: Equal
      value: "true"
      effect: NoSchedule
    - key: node-role.kubernetes.io/infra
      operator: Equal
      effect: NoSchedule
  CSI_PROVISIONER_TOLERATIONS: |-
    - key: node.ocs.openshift.io/storage
      operator: Equal
      value: "true"
      effect: NoSchedule
    - key: node-role.kubernetes.io/infra
      operator: Equal
      effect: NoSchedule
kind: ConfigMap
metadata:
  name: rook-ceph-operator-config
  namespace: openshift-storage

[root@grpi-ocp-hv00 openshift-storage]# cat OCSInitialization.yaml
apiVersion: ocs.openshift.io/v1
kind: OCSInitialization
```

```
metadata:
  name: ocsinit
  namespace: openshift-storage
spec:
  enableCephTools: true
```

I comandi utilizzati per eseguire l'installazione sono i seguenti:

Python

```
[root@grpi-ocp-hv00 openshift-storage]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 openshift-storage]# oc create -f namespace.yaml
operatorgroup.yaml subscription.yaml
```

Una volta creati gli oggetti, collegarsi alla dashboard di **ocp1-parallelo** e approvare l'installation plan che attende un'approvazione manuale.

Una volta disponibile l'operator proseguire con gli step successivi:

Python

```
[root@grpi-ocp-hv00 openshift-storage]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 openshift-storage]# oc create -f console-plugin.yaml
[root@grpi-ocp-hv00 openshift-storage]# oc create -f ocs-storage-cluster.yaml
[root@grpi-ocp-hv00 openshift-storage]# oc create -f rook-ceph-operator-config.yaml
[root@grpi-ocp-hv00 openshift-storage]# oc create -f OCSInitialization.yaml
```

Al termine verificare che tutti i pod all'interno del namespace **openshift-storage** siano *up&running* e che dalla dashboard lo stato dello storage system sia healthy.

3.2.6. Moving ingress su nodi infrastrutturali

All'interno della directory **/root/ocp-acm/policy-generator/ocp1-parallelo/ingress-conf** sono stati definiti i template necessari a spostare i router sui nodi infrastrutturali.

Per far questo sono stati preparati i seguenti template:

Python

```
[root@grpi-ocp-hv00 ingress-conf]# ll
-rw-r--r--. ingress-conf.yaml
-rw-r--r--. ingress.yaml
-rw-r--r--. kustomization.yaml

[root@grpi-ocp-hv00 ingress-conf]# cat kustomization.yaml
generators:
  - ingress-conf.yaml

[root@grpi-ocp-hv00 ingress-conf]# cat ingress-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-ingress-conf-ocp1
placementBindingDefaults:
  name: placement-binding-ingress-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-ingress-ocp1
    manifests:
      - path: ingress.yaml

[root@grpi-ocp-hv00 ingress-conf]# cat ingress.yaml
apiVersion: operator.openshift.io/v1
kind: IngressController
metadata:
  name: default
  namespace: openshift-ingress-operator
spec:
  nodePlacement:
    nodeSelector:
      matchLabels:
        node-role.kubernetes.io/infra: ""
    tolerations:
    - effect: NoSchedule
      key: node-role.kubernetes.io/infra
      operator: Exists
  replicas: 3
```

Le policy sono state create e applicate con il seguente comando:

Python

```
[root@grpi-ocp-hv00 ingress-conf]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it
```

```
[root@grpi-ocp-hv00 ingress-conf]# oc kustomize --enable-alpha-plugins=true . | oc
apply -f -
```

Al termine è possibile verificare che sul cluster **ocp1-parallelo**, i router risiedono, dopo il primo restart, sui nodi infrastrutturali.

3.2.7. Moving monitoring su nodi infrastrutturali

All'interno della directory **/root/ocp-acm/policy-generator/ocp1-parallelo/monitoring-conf** sono stati creati i template per spostare le componenti del monitoring sui nodi infrastrutturali, e per dare persistenza dei dati di *prometheus* e *alertmanager* tramite volumi non effimeri.

Seguono i template creati:

Python

```
[root@grpi-ocp-hv00 monitoring-conf]# ll
-rw-r--r--. kustomization.yaml
-rw-r--r--. monitoring-conf.yaml
-rw-r--r--. monitoring.yaml

[root@grpi-ocp-hv00 monitoring-conf]# cat kustomization.yaml
generators:
  - monitoring-conf.yaml

[root@grpi-ocp-hv00 monitoring-conf]# cat monitoring-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-monitoring-conf-ocp1
placementBindingDefaults:
  name: placement-binding-monitoring-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: mustonlyhave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-monitoring-ocp1
    manifests:
      - path: monitoring.yaml

[root@grpi-ocp-hv00 monitoring-conf]# cat monitoring.yaml
```

```
apiVersion: v1
data:
  config.yaml: |
    enableUserWorkload: true
    alertmanagerMain:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
      volumeClaimTemplate:
        spec:
          storageClassName: thin-csi
          resources:
            requests:
              storage: 20Gi
    grafana:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    k8sPrometheusAdapter:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    kubeStateMetrics:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    openshiftStateMetrics:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    prometheusK8s:
      retention: 30d
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
      volumeClaimTemplate:
        spec:
          storageClassName: thin-csi
          resources:
            requests:
              storage: 100Gi
    prometheusOperator:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
```

```
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    thanosQuerier:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    telemeterClient:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
kind: ConfigMap
metadata:
  name: cluster-monitoring-config
  namespace: openshift-monitoring
```

I template sono stati applicati con il comando seguente:

Python

```
[root@grpi-ocp-hv00 monitoring-conf]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 monitoring-conf]# oc kustomize --enable-alpha-plugins=true . |
oc apply -f -
```

3.2.8. Autenticazione tramite LDAP

All’interno della directory **/root/ocp-acm/policy-generator/ocp1-parallelo/oauth** sono stati definiti i template necessari a:

- Creare la *configmap* contenente la CA per l’utilizzo del protocollo ldaps nella comunicazione con il server LDAP
- Creare la secret contenente l’utenza per eseguire il bind all’LDAP e la password
- Configurare come metodo di autenticazione sul cluster, l’LDAP di Crédit Agricole

Python

```
[root@grpi-ocp-hv00 oauth]# ll
-rw-r--r--. auth-conf.yaml
-rw-r--r--. bind-secret.yaml
-rw-r--r--. kustomization.yaml
-rw-r--r--. cm-ca.yaml
```

```
-rw-r--r--. oauth.yaml

[root@grpi-ocp-hv00 oauth]# cat kustomization.yaml
generators:
  - auth-conf.yaml

[root@grpi-ocp-hv00 oauth]# cat auth-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-auth-conf-ocp1
placementBindingDefaults:
  name: placement-binding-auth-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-auth-conf-ocp1
    manifests:
      - path: oauth.yaml
  - name: policy-auth-cm-ca-ocp1
    manifests:
      - path: cm-ca.yaml
  - name: policy-auth-bind-secret-ocp1
    manifests:
      - path: bind-secret.yaml

[root@grpi-ocp-hv00 oauth]# cat bind-secret.yaml
apiVersion: v1
data:
  bindPassword: V004VEdTMjVXSjEzUXphMjEkUFI=
kind: Secret
metadata:
  name: ldap-secret
  namespace: openshift-config
type: Opaque

[root@grpi-ocp-hv00 oauth]# cat cm-ca.yaml
apiVersion: v1
data:
  ca.crt: |+
    -----BEGIN CERTIFICATE-----
    MIIFKjCCAxKgAwIBAgIQOLXqjbUkq5dN85ulGnvLPTANBgkqhkiG9w0BAQsFADAm
    MSQwIgYDVQQDExtDcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1QQVIwHhcNMTcwNTAy
    MTU0NDMxWhcNMzcwNTAyMTU1NDMwWjAmMSQwIgYDVQQDExtDcmVkaXRBZ3JpY29s
    ZUl0YWxpYVJDQS1QQVIwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQCh
    6zrpKWzle9HixD8Awnq0TnDC3tiDcv009WuWT5qb0PylqHmhjHy06vywNxV12OlV
    +GqWOfvxfJrf3+nWLir7nLxmf05732stWnK2ZK4hS4zaLkG/vt4IKZqkQSal3i1/
    /Ad1Pps8KbDXdgxZME1AxkBM6EbNU1RGoxjT/0xddbfJzZ7Ol5k4rsalM5vqIKfd
    bFBmyrtC7//YabRiUqYi19ulFFCXb4Wf4nu0rMwRhKynPrm+TooiSvDIyb0qEzIS
    3nOxn0ZjvUuL78AyikGWf70ay6tBol2OJTLCWc30tQPNK2CGznjdk45u24bV/X1F
    pGDq8XbdDDP8jnIMX/S/d4ABKcjOmL/cV1oNm5SfrI+E53EXyqW/rJnx40csWKwj
```

```
nFoItg8KUNEC9cgRR/7u/4OVHIiX065mqKef1HNHQGeNlqFPKEMqdWXDYLljw380
6g9VF4Wxq40JRN2QyzW++GpMAK88WfsxTbXx5GJ8mA1G/Zm/glPFniZGMDlx1IxS
jfZ/mXPTDdmact0PwCBT45P7EWcbdosFrnHf5qCo6z8QAUMJv0zlSN6orPOAWald
fZmpRfhyoQh+DeQ+IoTZ27E/mLm7lLkX1Ixj7Y+sQaAdQ3AjBtHyYgzmPYiI0TJO
3h63mZWrHXu22tqlTufSmZnQvHxGgiQ14Ruqv0NQIQIDAQABo1QwUjALBgNVHQ8E
BAMCAYYwEgYDVR0TAQH/BAgwBgEB/wIBATAdBgNVHQ4EFgQUN1a2wutAq3+PW3n2
AFnJxV7iTUEwEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQELBQADggIBAB7t
opTXqZhxm+3Fkg3vRoVozBqD1cPZ/NNFE70yKe+vsVXYg+QLfXZE24Uo0CYp/oRZ
9fJ2t80wIQ0KU2RPZq9Bpi6H37vkV5b6UI55SQZaLwCJfNHkouMqWVH6InfLVF2K
ARuPTEl33CvDN6sB+PT9IgUZtgpdjj/cCcMZS7v8LmDLFJlFmosEPnu2nTnadfVg
knlQ//cTiWHWM8ELyK3VnEDXHQqrFWSvjbd8trVi6pYP/aV07a1GWRctryJZGms7
yMVpW3q4dDK+kd0CerXurdsKuMJkzrcsqD73iPpZiGgilsj2N3iuBm99vwd93HVl
ha1Lvr1ZCkCL1f2J7iffxk9Wrm1GauFaO25ZydJ5UXu4ihgbnk6AYSK9h19IRc1r
PmLIghzpqLRXJpZjUa1b6Hytl0jookPbHPb0M6cCK35+L+fdetGXiLSZn4Y1vtqe
4rjHKa68Lkk4S+ljwz5DvbouCcHAgvOxTkX0M5fkClKS1E7gp2Eu3F8o31dmBlci
0kZQvFwHFdSNj3zIkxtoRE3TQD2I5CTzMkiURBD264ISjdwc8uKNHadILn1GyaXJ
lbNvnKb6w7hrcXCqHnTvl1mXu0MlX5zF+h+5mrpGezfEJuK7AlWyj/NsiMVjrVb2
TaSm5to8Jz08SkHyz2J5baoH0yx0g+AJKxRtnwqt
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIILDCCBhSgAwIBAgITKgAAAANLM56OzEXAcwAAAAAAAzANBgkqhkiG9w0BAQsF
ADAmMSQwIgYDVQQDExtDcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1QQVIwHhcNMTcw
NTAzMDkyODU5WhcNMjcwNTAzMDkzODU5WjBXMRIwEAYKCZImiZPyLGQBGRYCaXQx
GzAZBgoJkiaJk/IsZAEZFgtjYXJpcHJwY3BhcjEkMCIGA1UEAxMbQ3JlZGl0QWdy
aWNvbGVJdGFsaWFTQ0EtUEFSMIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKC
AgEAqtmT+HRBlIEG66OzYTzRENNO4Y2LW2CYyGpMIMHzpoAgTtRHQC1JbcKHE/+3
gyijkipPkbuYbrLea3zMbSgsJHwVasflXK+NufVE1412CFBoLBUUAEivh2zpBkmM
gOpYo/SvjGwCUuN7vVbraMGbflvDi27iKfMZgzK7hMNNO/ew+MNMqIVq/p95UC3L
Fx2TJtF6+pUEL1Tm06sWTniLk9PhL0s2re17U/mhz+QrGLsbqom4Zi+LrKB84TX0
Lis2iSCIIUT4piRccZDh3BF2TOkYrVlPFv1H3+bOpilzZVsSogzWy7I9sP/kDcqv
K3y2cLHRsckeQcuempJUj5bX+l6F9uDw80gMoBGRi/y2SF7doWQvoHuE2TTLRr0W
GAbGu2yy5GSO9i5l5i7sdouwi0MEhaYIsEvif68Q3Ja99PLjx1LvDcuIUKBu7hgm
uXuXkhMFUVjh8PdSIINpzG8wSPILpQC5uH3n6rGBCEBkqRjdmmLWADdgseU6ESMp
wT3ViDxSAg3zvWMF1v/H6hnOuBspnDGnUEbuY1JQjQP/aWn9+lfd8PGLem5S5DKL
Gb4vvWsw36tgoJpFQ6TqyV70z/hLMy8GFeWuOn8aU6NFAyzn56sPGY05KLwjDG+i
XuauPrl9pIvskvsJ69AkawbS6c2+fk1yBJw97g75EAuJsk8CAwEAAaOCAyAwggMc
MBIGCSsGAQQBgjcVAQQFAgMBAAEwIwYJKwYBBAGCNxUCBBYEFFnklte59RhxVuJM
auvEP4SuWNcHMB0GA1UdDgQWBBShy+zN34OTBRtsC41QwKHlT3KY5zAZBgkrBgEE
AYI3FAIEDB4KAFMAdQBiAEMAQTALBgNVHQ8EBAMCAYYwEgYDVR0TAQH/BAgwBgEB
/wIBADAfBgNVHSMEGDAWgBQ3VrbC60Crf49befYAWcnFXuJNQTCCAS0GA1UdHwSC
ASQwggEgMIIBHKCCARigggEUhoHLbGRhcDovLy9DTj1DcmVkaXRBZ3JpY29sZUl0
YWxpYVJDQS1QQVIsQ049R1JQSS1DQUEtSFYzMSxDTj1DRFAsQ049UHVibGljJTIw
S2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1D
QVJJUFJQQ1BBUixEQz1pdD9jZXJ0aWZpY2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/
b2JqZWN0Q2xhc3M9Y1JMRGlzdHJpYnV0aW9uUG9pbnSGRGh0dHA6Ly9wa2kuY2Fy
aXBycGNwYXIuaXQvQ2VydEVucm9sbC9DcmVkaXRBZ3JpY29sZUl0YWxpYVJDQS1Q
QVIuY3JsMIIBMgYIKwYBBQUHAQEEggEkMIIBIDCBvQYIKwYBBQUHMAKGgbBsZGFw
Oi8vL0NOPUNyZWRpdEFncmljb2xlSXRhbGlhUkNBLVBBUixDTj1BSUEsQ049UHVi
bGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmlndXJhdGlv
bixEQz1DQVJJUFJQQ1BBUixEQz1pdD9jQUNlcnRpZmljYXRlP2Jhc2U/b2JqZWN0
Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTBeBggrBgEFBQcwAoZSaHR0cDov
L3BraS5jYXJpcHJwY3Bhci5pdC9DZXJ0RW5yb2xsL0dSUEktQ0FBLUhWMzFfQ3Jl
ZGl0QWdyaWNvbGVJdGFsaWFSQ0EtUEFSLmNydDANBgkqhkiG9w0BAQsFAAOCAgEA
XbBUDlc4FeCJGdJeWWDvgK2brxO9VshgjgZV9GGmmFlLR/TKim0VkrRAjfSvxf1x
nto8bHZ2ivxBr0RSBVOXEvVYycMIkMxpbGbKAIkN2PnuMO5FCudNYpMA4P0HcQch
wiGQlonj7e2/Azvtyc5ML4xLubb6JQNt1L/76dCdheGmdYj3YNkrIzaDkMe3jZmW
TrVI+hOLOL9XuOnNzQkhZ0INQ/QQmUGQ6xdaM1z5MVkOvTPpkzhD8s6Vt/nkodOA
```

```
    J9gQEDlhO46tl67QqplsA8jX3wgRqvffZ3E9ZSx3t1dDsnslhsZEoDHVALTMcyfU
    EMEsGtRlkWPrUcEPzBnn9mTegaoEAby53OAVaW5FeT2iGSlCIhukiu70Mvf8MIAA
    /p3kDl2J3OtUJ/THjg8952JCa8WBpvON25cV4QU0PhfJmnBfoVHYmpAntcXcECS1
    OHJnkD0pRgqKz+GcW7mIVWrygaXwH+nXrJw22ympf+s2h3xvjPqFCy5PxDjZIyaP
    OD2S8PIWHfQZTztYhhsTl675U6oGO3T5/BRxQ+s+AKtjUpQ24Wz52tdulD9Ya1Xc
    f6Msid7qH9Nv9lT5sjyy+bNdla2YFvXcjEIh7g8GVqRWszkbbb2irU0f5PbjiApV
    Yv4sy+JZ53ZzY07YmIHBlvFPlm4194MNTBgbpd+zBHE=
    -----END CERTIFICATE-----
kind: ConfigMap
metadata:
  name: ca-config-map
  namespace: openshift-config

[root@grpi-ocp-hv00 oauth]# cat oauth.yaml
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
  - ldap:
      attributes:
        email:
        - mail
        id:
        - dn
        name:
        - cn
        preferredUsername:
        - sAMAccountName
      bindDN:
CN=cp_4462_ocp_ldap,OU=OU-UTENTI-SERVIZI,OU=OU-UTENTI,DC=cariprpcpar,DC=it
      bindPassword:
        name: ldap-secret
      ca:
        name: ca-config-map
      insecure: false
      url:
ldaps://msad0par.cariprpcpar.it/DC=cariprpcpar,DC=it?sAMAccountName?sub?(&(objectCl
ass=user)(|(memberOf=CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_DTR_USER,CN=User
s,DC=cariprpcpar,DC=it)(memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it)(mem
berOf=CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it)))
    mappingMethod: claim
    name: ldap
    type: LDAP
```

Per configurare l’operator dell’autenticazione è necessario eseguire il seguente comando:

Python

```
[root@grpi-ocp-hv00 oauth]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it
```

```
[root@grpi-ocp-hv00 oauth]# oc kustomize --enable-alpha-plugin=true . | oc apply -f
-
```

Attendere il riavvio dei pod dell'autenticazione prima di testare la login tramite LDAP.

3.2.9. Sync gruppi di utenti tra alberatura LDAP e OCP

All'interno della directory **/root/ocp-acm/policy-generator/ocp1-parallelo/group-sync-operator** sono stati definiti i template necessari a:

- Creare il namespace che ospita il group-sync-operator
- Installare il group-sync-operator
- Creare la *configmap* contenente la CA per l'utilizzo del protocollo ldaps nella comunicazione con il server LDAP: il campo ca.crt contiene il *base64encode* della CA.
- Creare la secret contenente l'utenza per eseguire il bind all'LDAP e la password
- Configurare il group sync operator
- Associare il ruolo cluster-admin agli utenti appartenenti al gruppo CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it

Python

```
[root@grpi-ocp-hv00 group-sync-operator]# ll
-rw-r--r--. group-sync-conf.yaml
-rw-r--r--. ldap-ca-bundle-group-sync.yaml
-rw-r--r--. ldap-creds-group-sync.yaml
-rw-r--r--. ldap-groupsync.yaml
-rw-r--r--. namespace.yaml
-rw-r--r--. operatorgroup.yaml
-rw-r--r--. role-bindig.yaml
-rw-r--r--. subscription.yaml
-rw-r--r--. kustomization.yaml


[root@grpi-ocp-hv00 group-sync-operator]# cat kustomization.yaml
generators:
  - group-sync-conf.yaml

[root@grpi-ocp-hv00 group-sync-operator]# cat group-sync-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-group-sync-conf-ocp1
placementBindingDefaults:
  name: placement-binding-group-sync-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-group-sync-namespace-ocp1
    manifests:
      - path: namespace.yaml
  - name: policy-group-sync-operatorgroup-ocp1
    manifests:
      - path: operatorgroup.yaml
  - name: policy-group-sync-subscription-ocp1
    manifests:
      - path: subscription.yaml
  - name: policy-group-sync-ldap-groupsync-ocp1
    manifests:
      - path: ldap-groupsync.yaml
  - name: policy-group-sync-ca-secret-ocp1
    manifests:
      - path: ldap-ca-bundle-group-sync.yaml
  - name: policy-group-sync-bind-secret-ocp1
    manifests:
      - path: ldap-creds-group-sync.yaml
  - name: policy-group-sync-admin-ocp1
    manifests:
      - path: role-bindig.yaml

[root@grpi-ocp-hv00 group-sync-operator]# cat namespace.yaml
apiVersion: v1
kind: Namespace
metadata:
  name: group-sync-operator
spec:
  finalizers:
  - kubernetes

[root@grpi-ocp-hv00 group-sync-operator]# cat operatorgroup.yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: group-sync-operator
  namespace: group-sync-operator
spec:
  targetNamespaces:
  - group-sync-operator

[root@grpi-ocp-hv00 group-sync-operator]# cat subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: group-sync-operator
  namespace: group-sync-operator
spec:
  channel: alpha
  installPlanApproval: Manual
  name: group-sync-operator
  source: community-operators
  sourceNamespace: openshift-marketplace

[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-groupsync.yaml
apiVersion: redhatcop.redhat.io/v1alpha1
kind: GroupSync
metadata:
  name: ldap-groupsync
  namespace: group-sync-operator
spec:
  providers:
  - ldap:
      activeDirectory:
        groupMembershipAttributes:
        - memberOf
        userNameAttributes:
        - sAMAccountName
        usersQuery:
          baseDN: DC=cariprpcpar,DC=it
          derefAliases: never
          filter:
(&(objectClass=user)(|(memberOf=CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_DTR_U
SER,CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar
,DC=it)(memberOf=CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it)))
          pageSize: 0
          scope: sub
      caSecret:
        kind: Secret
        name: ldap-ca-bundle-group-sync
        namespace: group-sync-operator
      credentialsSecret:
        kind: Secret
        name: ldap-creds-group-sync
        namespace: group-sync-operator
      insecure: false
      url: ldaps://msad0par.cariprpcpar.it
      whitelist:
      - CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_DTR_USER,CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it
      - CN=GU_OCP_USER,CN=Users,DC=cariprpcpar,DC=it
    name: ldap-group-sync
  schedule: '*/5 * * * *'

[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-ca-bundle-group-sync.yaml
apiVersion: v1
data:
  ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0tLS0tCk1JSUZLakNDQXhLZ0F3SUJBZ0lRT0xYcWpiVWtxNWROODV
1bEdudkxQVEFOQmdrcWhraUc5dzBCQVFzRkFEQW0KTVNRd0lnWURWUVFERXh0RGNtVmthWFJCWjNKcFkyOX
NaVWwwWVd4cFlWSkRRUzFRUVZJd0hoY05NVGN3TlRBeQpNVFUwTkRNeFdoY05NemN3TlRBeU1UVTFORE13V
2pBbU1TUXdJZ1lEVlFREV4dERjbVZrYVhSQlozSnBZMjlzClpVbDBZV3hwWVZKRFFTMVFRVkl3Z2dJaU1B
MEdDU3FHU0liM0RRRUJBUVVBQTRJQ0R3QXdnZ0lLQW9JQ0FRQ2gKNnpycEtXemxlOUhpeEQ4QXducTBUbkR
DM3RpRGN2MDA5V3VXVDVxYjBQeWxxSG1oakh5MDZ2eXdOeFYxMk9sVgorR3FXT2Z2eGZKcmYzK25XTGlyN2
5MeG1mMDU3MzJzdFduSzJaSzRoUzR6YUxrRy92dDRJS1pxa1FTYWwzaTEvCi9BZDFQcHM4S2JEWGRneFpNR
TFBeGtCTTZFYk5VMVJHb3hqVC8weGRkYmZKelo3T2w1azRyc2FsTTV2cUlLZmQKYkZCbXlydEM3Ly9ZYWJS
aVVxWWkxOXVsRkZDWGI0V2Y0bnUwck13UmhLeW5Qcm0rVG9vaVN2REl5YjBxRXpJUwozbk94bjBaanZVdUw
```

```
3OEF5aWtHV2Y3MGF5NnRCb2wyT0pUTENXYzMwdFFQTksyQ0d6bmpkazQ1dTI0YlYvWDFGCnBHRHE4WGJkRE
RQOGpuSU1YL1MvZDRBQktjak9tTC9jVjFvTm01U2ZySStFNTNFWHlxVy9ySm54NDBjc1dLd2oKbkZvSXRnO
EtVTkVDOWNnUlIvN3UvNE9WSElpWDA2NW1xS2VmMUhOSFFHZU5scUZQS0VNcWRXWERZTGxqdzM4MAo2ZzlW
RjRXeHE0MEpSTjJReXpXKytHcE1BSzg4V2ZzeFRiWHg1R0o4bUExRy9abS9nbFBGbmlaR01EbHgxSXhTCmp
mWi9tWFBURGRtYWN0MFB3Q0JUNDVQN0VXY2Jkb3NGcm5IZjVxQ282ejhRQVVNSnYwemxTTjZvclBPQVdhbG
QKZlptcFJmaHlvUWgrRGVRK0lvVFoyN0UvbUxtN2xMa1gxSXhqN1krc1FhQWRRM0FqQnRIeVlnem1QWWlJM
FRKTwozaDYzbVpXckhYdTIydHFsVHVmU21ablF2SHhHZ2lRMTRSdXF2ME5RSVFJREFRQUJvMVF3VWpBTEJn
TlZIUThFCkJBTUNBWVl3RWdZRFZSMFRBUUgvQkFnd0JnRUIvd0lCQVRBZEJnTlZIUTRFRmdRVU4xYTJ3dXR
BcTMrUFczbjIKQUZuSnhWN2lUVUV3RUFZSkt3WUJCQUdDTnhVQkJBTUNBUUF3RFFZSktvWklodmNOQVFFTE
JRQURnZ0lCQUI3dApvcFRYcVpoeG0rM0ZrZzN2Um9Wb3pCcUQxY1BaL05ORkU3MHlLZSt2c1ZYWWcrUUxmW
FpFMjRVbzBDWXAvb1JaCjlmSjJ0ODB3SVEwS1UyUlBacTlCcGk2SDM3dmtWNWI2VUk1NVNRWmFMd0NKZk5I
a291TXFXVkg2SW5mTFZGMksKQVJ1UFRFbDMzQ3ZETjZzQitQVDlJZ1VadGdwZGpqL2NDY01aUzd2OExtREx
GSmxGbW9zRVBudTJuVG5hZGZWZwprbmxRLy9jVGlXSFdNOEVMeUszVm5FRFhIUXFyRldTdmpiZDh0clZpNn
BZUC9hVjA3YTFHV1JjdHJ5SlpHbXM3CnlNVnBXM3E0ZERLK2tkMENlclh1cmRzS3VNSmt6cmNzcUQ3M2lQc
FppR2dpbHNqMk4zaXVCbTk5dndkOTNIVmwKaGExTHZyMVpDa0NMMWYySjdpZmZ4azlXcm0xR2F1RmFPMjVa
eWRKNVVYdTRpaGdibms2QVlTSzloMTlJUmMxcgpQbUxJZ2h6cHFMUlhKcFpqVWExYjZIeXRsMGpvb2tQYkh
QYjBNNmNDSzM1K0wrZmRldEdYaUxTWm40WTF2dHFlCjRyakhLYTY4TGtrNFMrbGp3ejVEdmJvdUNjSEFndk
94VGtYME01ZmtDbEtTMUU3Z3AyRXUzRjhvMzFkbUJsY2kKMGtaUXZGd0hGZFNOajN6SWt4dG9SRTNUUUQyS
TVDVHpNa2lVUkJEMjY0SVNqZHdjOHVLTkhhZElMbjFHeWFYSgpsYk52bktiNnc3aHJjWENxSG5UdmwxbVh1
ME1sWDV6RitoKzVtcnBHZXpmRUp1SzdBbFd5ai9Oc2lNVmpyVmIyClRhU201dG84SnowOFNrSHl6Mko1YmF
vSDB5eDBnK0FKS3hSdG53cXQKLS0tLS1FTkQgQ0VSVElGSUNBVEUtLS0tLQotLS0tLUJFR0lOIENFUlRJRk
lDQVRFLS0tLS0KTUlJSUxEQ0NCaFNnQXdJQkFnSVRLZ0FBQUFOTE01Nk96RVhBY3dBQUFBQUFBekFOQmdrc
WhraUc5dzBCQVFzRgpBREFtTVNRd0lnWURWUVFERXh0RGNtVmthWFJCWjNKcFkyOXNaVWwwWVd4cFlWSkRR
UzFRUVZZJd0hoY05VGN3Ck5UQXpNRGt5T0RVNVdoY05NamN3TlRBek1Ea3pPRFU1V2pCWE1SSXdFQVlLQ1p
JbWlaUHlMR1FCR1JZQ2FYUXgKR3pBWkJnb0praWFKay9Jc1pBRVpGZ3RqWVhKcGNISSndZM0JoY2pFa01DSU
dBMVVFQXhNYlEzSmxaR2wwUVdkeQphV052YkdWSmRHRnNhV0ZUUTBFdFVFRlNNSUlDSWpBTkJna3Foa2lHO
XcwQkFRRUZBQU9DQWc4QU1JSUNDZ0tDCkFnRUFxdG1UK0hSQmxJRUc2Nk96WVR6UkVOTk80WTJMVzJDWXlH
cE1JTUh6cG9BZ1R0UkhRQzFKYmNLSEUvKzMKZ3lpamtpcFBrYnVZYnJMZWEzek1iU2dzSkh3VmFzZmxYSyt
OdWZWRTE0MTJDRkJvTEJVVUFFaXZoMnpwQmttTQpnT3BZby9TdmpHd0NVdU43dlZicmFNR2JmbHZEaTI3aU
tmTVpneks3aE1OTk8vZXcrTU5cUlWcS9wOTVVQzNMCkZ4M1RKdEY2K3BVRUwxVG0wNnNXVG5pTGs5UGhMM
HMycmUxN1UvbWh6K1FyR0xzYnFvbTRaaStMcktCODRUWDAKTGlzMml0Q0lJVVQ0cGlSY2NaRGgzQkYyVE9r
WXJWbFBGdjFIMytiT3BpbHpaVnNTb2d6V3k3STlzUC9rRGNxdgpsLM3kyY0xIUnNja2VRY3VlbXBKVWo1Ylg
rbDZGOXVEdzgwZ01vQkdSaS95MlNGN2RvV1F2b0h1RTJUVExxScjBXCkdBYkd1Mnl5NUdTTzlpNWw1aTdzZG
91d2kwTUVoYVlJc0V2aWY2OFEzSmE5OVBMangxTHZEY3VJVUtCdTdoZ20KdVh1WGtoTUZVVmpoOFBkU0lJT
nB6Rzh3U1BJTHBRQzV1SDNuNnJHQkNFQmtxUmpkbW1MV0FEZGdzZVU2RVNNcAp3VDNWaUR4U0FnM3p2V01G
MXYvSDZobk91QnNwbkRHblVFYnVZMUpRalFQL2FXbjkrbGZkOFBHTGVtNVM1REtMCkdiNHZ2V3N3MzZ0Z29
KcEZRNlRxeVY3MHovaExxNeThHRmVXdU9uOGFVNk5GQXl6bjU2c1BHWTA1S0x3akRHK2kKWHVhdVBybDlwSX
Zza3ZzSjY5QWthd2JTNmMyK2ZrMXlCSnc5N2c3NUVBdUpzazhDQXdFQUFhT0NBeUF3ZDZZwpNQklHQ1NzR
0FRUUJnamNWQVFRRkFnTUJBQUV3SXdZSktvWklodmNOQVFVG5rbHRlNTlSaHhWdUpNCmF1dkVQ
NFN1V05jSE1CMEdBMVVkRGdRV0JCU2h5K3pOMzRPVEJSdHNDNDFRd0tIbFQzS1k1ekFaQmdrckJnRUUKQVl
JM0ZBSUVEQjRLQUZNQWRRQmlBRU1BUVRBTEJnTlZIUThFQkFNQ0FZWXdFZ1lEVlIwVEFRSC9CQWd3QmdFQg
ovd0lCQURBZkJnTlZIU01FR0RBV2dCUTNNWcmJDNjBDcmY0OWJlZllBV2NuRlh1Sk5RVENDQVMwR0ExVWRId
1NDkFTUXdnZ0VnTUlJQkhLQ0NBUmlnZ2dFVWhvSExiR1JoY0Y0Rvdkx5OURUajFEY21Wa2FYUkJaM0pwWTI5
c1pVbDAKWVd4cFlWSkRRUzFRUVZZJc1EwNDlSMUpRU1MxRFFVVRXRTRll6TVN4RFRqMURSSkFzUTA0OVVIVml
iR2xqSlRJd1MlY1SlRJd1UyVnlkbWxqWlhNbDNDMUVwNDlVMlZ5ZG1salpYTXNRMDQ5UTI5dVptbG5kWEpoZE
dsdmJpeEVVRejFEClFWSkpVRkpRUTFCQ1lpVEJlVFJGwZEQ5alpYSjBhV1pwWTJGMFpWSmxkbTlqWVhScGIyN
U1hWE4wUDJKaGMyVS8KY1JKcVpXTjBRMnhoYzNNOVkxSk1SR2x6ZEhKcFluVjBhVzl1VUc5cGJuUT9RVFZER2dw
ZEhBNkx5OXdPdGmt1WTJGeQphWEJhRUJ5Y0RkOd1lYSXVhWFF2UTJWeWRFVnVjbTlzYkM5RGNtVmthWFJCWjNKcFk
yOXNaVWwwWVd4cFlWSkRRU1FVSEFRRUVnZ0VvTUlJQkpEQ0J6Z1lJS3dZQkJRVUhNQUtHZ2JGc2IyUndPaTh2
THpBnyBd3Q0ZDUnBWM0Y0TUpjYnVkZDd2R2xIQXhKYVQ5TE1OMDlJNXJVVEpGWjJwM3NoN0E5ZjVVMVdGbXlQ
bGFMSklxWHMrSVNJNkdwYXlmRkZIMU01VVNVWXNtM0pJa2pqOGNWZjV4MlJTckgzNUFYRVdmVk1MaUlQNWt1
RlNjTkdEOHRoQURBV2dBZW9vNTJSSUt6QTRhZGVhS0tzdHFHa2dDSmpVV2dzNFpNdVYxZmFobm1mNzlLM2Yz
WmRXOTVmPQ==
V2Vll5Y01Ja014cGJHYktBSWtOMlBudU1PNUZDdWROWXBNQTRQMEhjUWNoCndpR1Fsb25qN2UyL0F6dnR5Y
zVNTDR4THViYjZKUU50MUwvNzZkQ2RoZUdtZFlqM1lOa3JJemFEa01lM2pabVcKVHJWSStoT0xPTDlYdU9u
TnpRa2haMElOUS9RUW1VR1E2eGRhTTF6NU1Wa092VFBwa3poRDhzNlZ0L25rb2RPQQpKOWdRRURsaE80NnR
sNjdRcXBsc0E4algzd2dScXZmZlozRTlaU3gzdDFkRHNuc2xoc1pFb0RIVkFMVE1jeWZVCkVNRXNHdFJsa1
dQclVjRVB6Qm5uOW1UZWdhb0VBYnk1M09BVmFXNUZlVDJpR1NsQ0lodWtpdTcwTXZmOE1JQUEKL3Aza0RsM
kozT3RVSi9USGpnODk1MkpDYThXQnB2T04yNWNWNFFVMFBoZkptbkJmb1ZIWW1wQW50Y1hjRUNTMQpPSEpu
a0QwcFJncUt6K0djVzdtSVZXcnlnYVh3SCtuWHJKdzIyeW1wZitzMmgzeHZqUHFGQ3k1UHhEalpJeWFQCk9
EMlM4UElXSGZRWlR6dFloaHNUbDY3NVU2b0dPM1Q1L0JSeFErcytBS3RqVXBRMjRXejUydGR1bEQ5WWExWG
MKZjZNc2lkN3FIOU52OWxUNXNqeXkrYk5kbGEyWUZ2WGNqRUloN2c4R1ZxUldzemtiYmIyaXJVMGY1UGJqa
UFwVgpZdjRzeStKWjUzWnpZMDdZbUlIQmx2RlBsbTQxOTRNTlRCZ2JwZCt6QkhFPQotLS0tLUVORCBDRVJU
SUZJQ0FURS0tLS0tCg==
kind: Secret
metadata:
  name: ldap-ca-bundle-group-sync
  namespace: group-sync-operator
type: Opaque

[root@grpi-ocp-hv00 group-sync-operator]# cat ldap-creds-group-sync.yaml
apiVersion: v1
data:
  password: V004VEdTMjVXSjEzUXphMjEkUFI=
                                                                           username:
Q049Y3BfNDQ2Ml9vY3BfbGRhcCxPVT1PVS1VVEVOVEktU0VSVklaSSxPVT1PVS1VVEVOVEksREM9Y2FyaXB
ycGNwYXIsREM9aXQ=
kind: Secret
metadata:
  name: ldap-creds-group-sync
  namespace: group-sync-operator
type: Opaque

[root@grpi-ocp-hv00 group-sync-operator]# cat role-bindig.yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: clusteradmin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it
```

Per creare questa policy è stato lanciato il comando seguente:

```Python
[root@grpi-ocp-hv00 group-sync-operator]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 group-sync-operator]# oc kustomize --enable-alpha-plugin=true .
| oc apply -f -
```

IMPORTANTE: una volta creata la policy, collegarsi alla console di OCP, ed approvare a mano l'installation-plan dell'operator group-sync-operator.

3.2.10. Installazione componente di logging

All'interno della directory **/root/ocp-acm/policy-generator/ocp1-parallelo/logging-loki** sono stati creati i template necessari a:

- Installare l'operator openshift-logging
- Installare l'operator loki-operator
- Preparare i riferimenti al bucket S3 messo a disposizione dall'istanza interna di ODF
- Definire l'istanza di logging
- Define l'istanza di lokistack

Riporto i template creati a questo fine:

Python

```
[root@grpi-ocp-hv00 logging-loki]# cat kustomization.yaml
generators:
  - logging-loki-conf.yaml

[root@grpi-ocp-hv00 logging-loki]# cat logging-loki-conf.yaml
apiVersion: policy.open-cluster-management.io/v1
kind: PolicyGenerator
metadata:
  name: generator-logging-loki-conf-ocp1
placementBindingDefaults:
  name: placement-binding-logging-loki-conf-ocp1
policyDefaults:
  namespace: acm-hub-policy
  placement:
    clusterSelectors:
      name: ocp1-parallelo
  complianceType: musthave
  remediationAction: enforce
  severity: high
policies:
  - name: policy-logging-loki-namespace-ocp1
    manifests:
      - path: namespace.yaml
  - name: policy-logging-loki-operatorgroup-ocp1
    manifests:
      - path: operatorgroup.yaml
  - name: policy-logging-loki-subscription-ocp1
    manifests:
      - path: subscription.yaml
  - name: policy-logging-loki-operator-ocp1
    manifests:
      - path: loki-operator-openshift-operators-redhat.yaml
  - name: policy-logging-loki-sub-loki-ocp1
    manifests:
      - path: loki-subscription.yaml
  - name: policy-logging-loki-bucket-ocp1
    manifests:
      - path: loki-bucket-odf.yaml
  - name: policy-logging-loki-instance-ocp1
    manifests:
      - path: lokistack-instance.yaml
  - name: policy-logging-loki-cl-instance-ocp1
    manifests:
      - path: clusterlogging-instance.yaml
  - name: policy-logging-loki-secret-ocp1
    manifests:
      - path: logging-loki-odf-secret.yaml

[root@grpi-ocp-hv00 logging-loki]# cat namespace.yaml
apiVersion: v1
kind: Namespace
metadata:
  name: openshift-logging
spec:
  finalizers:
  - kubernetes

[root@grpi-ocp-hv00 logging-loki]# cat operatorgroup.yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: openshift-logging
  namespace: openshift-logging
spec:
  targetNamespaces:
  - openshift-logging

[root@grpi-ocp-hv00 logging-loki]# cat subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: cluster-logging
  namespace: openshift-logging
spec:
  channel: stable
  installPlanApproval: Manual
  name: cluster-logging
  source: redhat-operators
  sourceNamespace: openshift-marketplace

[root@grpi-ocp-hv00 logging-loki]# cat
loki-operator-openshift-operators-redhat.yaml
apiVersion: operators.coreos.com/v1
kind: Operator
metadata:
  name: loki-operator.openshift-operators-redhat
spec: {}

[root@grpi-ocp-hv00 logging-loki]# cat loki-subscription.yaml
```

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: loki-operator
  namespace: openshift-operators-redhat
spec:
  channel: stable
  name: loki-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
  installPlanApproval: Manual

[root@grpi-ocp-hv00 logging-loki]# cat loki-bucket-odf.yaml
apiVersion: objectbucket.io/v1alpha1
kind: ObjectBucketClaim
metadata:
  name: loki-bucket-odf
  namespace: openshift-logging
spec:
  generateBucketName: loki-bucket-odf
  objectBucketName: obc-openshift-logging-loki-bucket-odf
  storageClassName: openshift-storage.noobaa.io

[root@grpi-ocp-hv00 logging-loki]# cat lokistack-instance.yaml
apiVersion: loki.grafana.com/v1
kind: LokiStack
metadata:
  name: logging-loki
  namespace: openshift-logging
spec:
  limits:
    global:
      retention:
        days: 10
  managementState: Managed
  size: 1x.extra-small
  storage:
    schemas:
    - effectiveDate: "2024-04-05"
      version: v12
    secret:
      name: logging-loki-odf
      type: s3
    tls:
      caName: openshift-service-ca.crt
  storageClassName: ocs-storagecluster-ceph-rbd
  template:
    compactor:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    distributor:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    gateway:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    indexGateway:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    ingester:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    querier:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    queryFrontend:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
    ruler:
      nodeSelector:
        node-role.kubernetes.io/infra: ""
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/infra
  tenants:
    mode: openshift-logging

[root@grpi-ocp-hv00 logging-loki]# cat clusterlogging-instance.yaml
apiVersion: logging.openshift.io/v1
kind: ClusterLogging
metadata:
  name: instance
  namespace: openshift-logging
spec:
  collection:
    tolerations:
    - effect: NoSchedule
      key: node-role.kubernetes.io/infra
    - effect: NoSchedule
      key: node.ocs.openshift.io/storage
      value: "true"
    type: vector
  logStore:
    lokistack:
      name: logging-loki
    type: lokistack
  managementState: Managed
  visualization:
    type: ocp-console

[root@grpi-ocp-hv00 logging-loki]# cat logging-loki-odf-secret.yaml
apiVersion: v1
data:
  access_key_id: WnBnNHEzZ21mRmJYSWJVVFlVb3A=
  access_key_secret: YzNxSC83ZXBHOXQ4S2RiWGRkc0VTeU1FdFJGUGtQTU94QzliUlF5dQ==
  bucketnames:
bG9raS1idWNrZXQtb2RmLTE2MGE5OThjLTdiYmQtNDFiYy04ZmI2LTkwMzAyMmU2NDhjMAo=
  endpoint: aHR0cHM6Ly9zMy5vcGVuc2hpZnQtc3RvcmFnZS5zdmM6NDQz
kind: Secret
metadata:
  name: logging-loki-odf
  namespace: openshift-logging
type: Opaque
```

La secret **logging-loki-odf** è stata creata eseguendo il base64encode di:

- Access-key creata con l'objectbucketclaim
- Access-key-secret creata con l'objectbucketclaim
- Il nome del bucket S3 creato
- Il nome dell'endpoint che fornisce l'S3

A questo punto è possibile eseguire l'installazione di tutte le componenti del logging eseguendo il seguente comando:

```
Python
[root@grpi-ocp-hv00 logging-loki]# oc login -u USERNAME -p PASSWORD
https://api.ocp-parallelo.cariprpcpar.it

[root@grpi-ocp-hv00 logging-loki]# oc kustomize --enable-alpha-plugin=true . | oc
apply -f -
```

Una volta lanciato il comando è necessario collegarsi alla console di ocp1-parallelo ed approvare manualmente l'installation plan per le subscription di loki e del cluster logging.

3.2.11. Installazione Quay

All’interno della directory **/root/ocp-acm/cluster-template** è stata creata la directory **quay-installation**, suddivisa a sua volta in due directory che contengono i template dell’operator necessari ad eseguire il deploy della componente **QuayRegistry**

Come deciso in fase preliminare l’istanza Quay **non** ospiterà le componenti:

- Scanning
- Mirroring

L’operator si occuperà invece di procedere alla creazione e gestione “**managed**” delle seguenti componenti:

- Crittografia
- ObjectBucketClaim
- Monitoring
- Quay
- HPA
- Redis
- Quay PostgreSQL

3.2.11.1. Quay Operator

Riporto i template della componente Quay operator:

```
[root@grpi-ocp-hv00 quay-namespace]# ll
-rw-r--r--. kustomization.yaml
-rw-r--r--. 0-namespace.yaml

[root@grpi-ocp-hv00 quay-installation] # ll
-rw-r--r--. kustomization.yaml
-rw-r--r--. 6-quayregistry.yaml
-rw-r--r--. 5-secret-ac-qy-extra-ca-certs-46f8b28mk5.yaml
-rw-r--r--. 4-secret-ac-qy-config-bundle-hcr89.yaml
-rw-r--r--. 3-subscription.yaml
-rw-r--r--. 2-ac-qy-quay-postgres-13-pvc.yaml
-rw-r--r--. 1-operator-group.yaml

[root@grpi-ocp-hv00 quay-installation] # cat quay-namespace/kustomization.yaml
resources:
- 0-namespace.yaml
generatorOptions:
  disableNameSuffixHash: true

[root@grpi-ocp-hv00 quay-installation] # cat quay-namespace/0-namespace.yaml
```

```
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  annotations:
    openshift.io/node-selector: node-role.kubernetes.io/infra=
    scheduler.alpha.kubernetes.io/defaultTolerations: '[{"operator": "Exists", "effect":
      "NoSchedule", "key": "node-role.kubernetes.io/infra"} ]'
  name: registry
spec:
 {}

[root@grpi-ocp-hv00 quay-installation] # cat quay-template/kustomization.yaml
resources:
- 1-operator-group.yaml
- 2-ac-qy-quay-postgres-13-pvc.yaml
- 3-subscription.yaml
- 4-secret-ac-qy-config-bundle-hcr89.yaml
- 5-secret-ac-qy-extra-ca-certs-46f8b28mk5.yaml
- 6-quayregistry.yaml
generatorOptions:
  disableNameSuffixHash: true

[root@grpi-ocp-hv00 quay-installation] # cat quay-template/1-operator-group.yaml
apiVersion: operators.coreos.com/v1
kind: OperatorGroup
metadata:
  name: ac-knjr2
  namespace: registry
spec:

[root@grpi-ocp-hv00 quay-installation] # cat quay-template/2-ac-qy-quay-postgres-13-pvc.yaml
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    quay-buildmanager-hostname: ""
    quay-component: postgres
    quay-operator-service-endpoint: http://quay-operator.registry.svc.cluster.local:7071
    quay-registry-hostname: ac-quay-registry.apps.ocp1-parallelo.cariprpcar.it
    volume.beta.kubernetes.io/storage-provisioner: openshift-storage.rbd.csi.ceph.com
    volume.kubernetes.io/storage-provisioner: openshift-storage.rbd.csi.ceph.com
  labels:
    quay-component: postgres
    quay-operator/quayregistry: ac
  name: ac-quay-postgres-13
  namespace: registry
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 50Gi
  storageClassName: ocs-storagecluster-ceph-rbd

[root@grpi-ocp-hv00 quay-installation] # cat quay-template/3-subscription.yaml
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: quay-operator
  namespace: registry
spec:
  channel: stable-3.11
  installPlanApproval: Manual
  name: quay-operator
  source: redhat-operators
  sourceNamespace: openshift-marketplace
  startingCSV: quay-operator.v3.11.0

[root@grpi-ocp-hv00 quay-installation] # cat
quay-template/4-secret-ac-qy-config-bundle-hcr89.yaml
apiVersion: v1
data:
  config.yaml: QUxMT1dfUFVMTFNfV…(hidden)..AtIENOPVVzZXJzCg==
kind: Secret
metadata:
  name: ac-config-bundle-hcr89
  namespace: registry
type: Opaque

[root@grpi-ocp-hv00 quay-installation] # cat
quay-template/5-secret-ac-qy-extra-ca-certs-46f8b28mk5.yaml
apiVersion: v1
data:
  custom-ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0t…(hidden)..TlRCZ2JwZCt6QkhFPQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0t
Cg==
kind: Secret
metadata:
  annotations:
    quay-buildmanager-hostname: ""
    quay-operator-service-endpoint: http://quay-operator.registry.svc.cluster.local:7071
    quay-registry-hostname: ac-quay-registry.apps.ocp1-parallelo.cariprpcar.it
  labels:
    quay-operator/quayregistry: ac
  name: ac-extra-ca-certs-46f8b28mk5
  namespace: registry
type: Opaque
```

```
[root@grpi-ocp-hv00 quay-installation] # cat quay-template/6-quayregistry.yaml
apiVersion: quay.redhat.com/v1
kind: QuayRegistry
metadata:
  name: ac
  namespace: registry
spec:
  components:
  - kind: clair
    managed: false
  - kind: postgres
    managed: true
  - kind: objectstorage
    managed: true
  - kind: redis
    managed: true
  - kind: horizontalpodautoscaler
    managed: true
  - kind: route
    managed: true
  - kind: mirror
    managed: false
  - kind: monitoring
    managed: true
  - kind: tls
    managed: true
  - kind: quay
    managed: true
    overrides:
      resources:
        limits:
          cpu: "4"
          memory: 16Gi
        requests:
          cpu: "2"
          memory: 8Gi
  - kind: clairpostgres
    managed: false
  configBundleSecret: ac-config-bundle-hcr89
```

Per installare l’operator di **Quay** sono stati eseguiti i seguenti comandi:

```
[root@grpi-ocp-hv00 quay-namespace]# oc login -u USERNAME -p PASSWORD
https://api.ocp1-parallelo.cariprpcpar.it
[root@grpi-ocp-hv00 quay-namespace]# oc apply -k .
[root@grpi-ocp-hv00 quay-template]# oc apply -k .
```

A questo punto è necessario collegarsi alla dashboard ed eseguire manualmente l’approvazione dell’installation plan.

I template utilizzati garantiscono una configurazione finale del prodotto come desiderato, a partire dalla schedulazione all’interno dei nodi “**infra**” e **Day 2** come **configurazione LDAP** e **features Quay.**

3.2.11.2. Schedulazione all’interno dei nodi infra

La schedulazione di tutti gli oggetti dell’operator **Quay** sono garantiti dalla presenza delle annotations all’interno del namespace “**registry**” dedicato ad ospitarli. Nello specifico possiamo osservare il template **0-namespace.yaml** presente all’interno della directory **quay-namespace:**

```
[root@grpi-ocp-hv00 quay-installation] # cat quay-namespace/0-namespace.yaml
apiVersion: project.openshift.io/v1
kind: Project
metadata:
  annotations:
    openshift.io/node-selector: node-role.kubernetes.io/infra=
    scheduler.alpha.kubernetes.io/defaultTolerations: '[{"operator": "Exists", "effect":
      "NoSchedule", "key": "node-role.kubernetes.io/infra"} ]'
  name: registry
spec:
 {}
```

Le **annotations** evidenziate sopra garantiscono rispettivamente:

- **Selettore** utile alla schedulazione dei pod all’interno dei nodi infra
- **Toleration** utile a garantire che la **Taint** presente sui nodi venga tollerata e la schedulazione avvenga con esito positivo

3.2.11.3. Storage PostgreSQL

Utile a storicizzare i **metadata** dei file, il database utile alle istanze **Quay** necessita di uno **storage permanente** da dedicare all’istanza **PostgreSQL**. Data la necessità di ospitare tale volume all’interno di **ODF** e non del default verso **vSphere**, si è optato per rendere tale creazione prerequisito utile alla messa campo dell’istanza attraverso la definizione dell’oggetto **PersistentVolumeClaim** anch’esso curato tramite ordine apposito del **Kustomization.**

La definizione dell’oggetto interessato è recuperabile all’interno del file **2-ac-qy-quay-postgres-13-pvc.yaml:**

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  annotations:
    quay-buildmanager-hostname: ""
    quay-component: postgres
    quay-operator-service-endpoint: http://quay-operator.registry.svc.cluster.local:7071
    quay-registry-hostname: ac-quay-registry.apps.ocp1-parallelo.cariprpcar.it
    volume.beta.kubernetes.io/storage-provisioner: openshift-storage.rbd.csi.ceph.com
    volume.kubernetes.io/storage-provisioner: openshift-storage.rbd.csi.ceph.com
  labels:
    quay-component: postgres
    quay-operator/quayregistry: ac
  name: ac-quay-postgres-13
  namespace: registry
spec:
  accessModes:
  - ReadWriteOnce
  resources:
    requests:
      storage: 50Gi
  storageClassName: ocs-storagecluster-ceph-rbd
```

3.2.11.4. Autenticazione LDAP

La configurazione LDAP viene garantita in fase di installazione dell'operator attraverso il passaggio del **config-bundle-secret** contenente il blocco dedicato alla sua configurazione.

Tale secret viene definita come prerequisito in ordine di deploy **quay-template/4-secret-ac-qy-config-bundle-hcr89.yaml** utile a garantire che l'oggetto **QuayRegistry** venga deployato correttamente e con la configurazione LDAP già impostata al suo interno:

```
AUTHENTICATION_TYPE: LDAP
LDAP_ADMIN_DN: CN=cp_4462_ocp_ldap,OU=OU-UTENTI-SERVIZI,OU=OU-UTENTI,DC=cariprpcpar,DC=it
LDAP_ADMIN_PASSWD: '..(hidden)..'
LDAP_ALLOW_INSECURE_FALLBACK: false
LDAP_BASE_DN:
    - DC=cariprpcpar
    - DC=it
LDAP_EMAIL_ATTR: userPrincipalName
LDAP_UID_ATTR: sAMAccountName
LDAP_URI: ldaps://cariprpcpar.it:3269
LDAP_USER_FILTER:
(|(memberOf=CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_DTR_USER,CN=Users,DC=cariprpcpar,DC=it
)(memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it)(memberOf=CN=GU_OCP_USER,CN=Users,DC=ca
riprpcpar,DC=it))
LDAP_SUPERUSER_FILTER: (memberOf=CN=GU_OCP_ADMIN,CN=Users,DC=cariprpcpar,DC=it)
LDAP_TIMEOUT: 30
LDAP_NETWORK_TIMEOUT: 30
FEATURE_UI_V2: true
LDAP_USERS_RDN:
    - CN=Users
```

Per permettere una comunicazione crittografata verso il server LDAP, è stato inoltre necessario aggiungere la **CA** all'interno degli **extra-certs**. Tale configurazione viene garantita come prerequisito nell'ordine di deploy del **Kustomization.**

Nello specifico il file di template che si occupa di tale creazione è il seguente **quay-template/5-secret-ac-qy-extra-ca-certs-46f8b28mk5.yaml** contenente il data **custom-ca.crt**:

```
apiVersion: v1
data:
  custom-ca.crt:
LS0tLS1CRUdJTiBDRVJUSUZJQ0FURS0t...(hidden)..TlRCZ2JwZCt6QkhFPQotLS0tLUVORCBDRVJUSUZJQ0FURS0tLS0
tCg==
kind: Secret
metadata:
  annotations:
    quay-buildmanager-hostname: ""
    quay-operator-service-endpoint: http://quay-operator.registry.svc.cluster.local:7071
    quay-registry-hostname: ac-quay-registry.apps.ocp1-parallelo.cariprpcar.it
  labels:
    quay-operator/quayregistry: ac
  name: ac-extra-ca-certs-46f8b28mk5
  namespace: registry
type: Opaque
```