Red Hat Identity Management (IdM) – Installation Guide

Document Version: 1.0

Author: Abhishek & Sachin

Date: 17-June-2025

Platform: Red Hat Enterprise Linux 9.3

Target: Bare-metal / VM deployment

1. Prerequisites

OS: Red Hat Enterprise Linux 9.3 (64-bit)

Hostname: idm.ocp4.example.com

IP Address: 192.168.50.40

DNS: Proper forward and reverse DNS entries

SELinux: Enforcing

Time Sync: NTP configured via chronyd

Package Source: Red Hat Subscription or local repo

Required Ports: 80, 443, 389, 636, 88, 464 (TCP/UDP), 123 UDP

2. System Preparation

Set hostname

hostnamectl set-hostname idm.ocp4.example.com

Update system

dnf update -y

Configure /etc/hosts

echo "192.168.50.40 idm.ocp4.example.com idm" >> /etc/hosts

Enable firewall and open necessary ports

firewall-cmd --permanent --zone=trusted --add-port={53,80,443,389,636,88,464}/tcp

firewall-cmd --permanent --zone=trusted --add-port={53,88,464,123}/udp

firewall-cmd --add-service=freeipa-4

firewall-cmd --add-service=dns

firewall-cmd --runtime-to-permanent

firewall-cmd --list-services
cockpit dhcpv6-client dns freeipa-4 ssh

firewall-cmd –reload

3. Install FreeIPA Server Packages

---

dnf install ipa-server ipa-server-dns –y

4. IPA Server Installation

---

ipa-server-install

Sample Interactive Answers:

Do you want to configure integrated DNS (BIND)? [no]: no

NetBIOS domain name [OCP4]: OCP4

Do you want to configure chrony with NTP server or pool address? [no]: [Enter]

Continue to configure the system with these values? [no]: yes

5. Post-Installation Checks

Verify services

ipactl status

Confirm admin login

kinit admin

ipa user-find

Web UI: https://idm.ocp4.example.com

Login: admin

6. LDAP & TLS Testing

---

ldapsearch -x -H ldaps://idm.ocp4.example.com \

-D "uid=admin,cn=users,cn=accounts,dc=ocp4,dc=example,dc=com" \

-W -b "cn=users,cn=accounts,dc=ocp4,dc=example,dc=com" "(uid=admin)"

7. Optional: Create User

---

ipa user-add goku --first=Goku --last=Son --email=goku@ocp4.example.com --password

8. Reference

Red Hat IdM Docs:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/installing_identity_management/index

OpenShift LDAP Identity Provider Integration

To integrate FreeIPA with OpenShift as an LDAP Identity Provider, follow the official documentation from Red Hat:

https://docs.redhat.com/en/documentation/openshift_container_platform/4.14/html/authentication_and_authorization/configuring-identity-providers#identity-provider-overview_configuring-ldap-identity-provider

Sample YAML for configuring LDAP as an Identity Provider in OpenShift:

```
apiVersion: config.openshift.io/v1
kind: OAuth
metadata:
  name: cluster
spec:
  identityProviders:
  - name: Red Hat Identity Management
    mappingMethod: claim
    type: LDAP
    ldap:
      url:
ldaps://idm.ocp4.example.com/cn=users,cn=accounts,dc=ocp4,dc=example,dc=com?uid
      bindDN: uid=admin,cn=users,cn=accounts,dc=ocp4,dc=example,dc=com
      bindPassword:
        name: abhi-ldap
      ca:
        name: abhi-cm
      insecure: false
      attributes:
        id: [uid]
        name: [cn]
        email: [mail]
        preferredUsername: [uid]
```

Make sure to create the associated secrets and configmaps (bind password and CA certificate) in the openshift-config namespace.