

Passcert

Higher Quality, better service!



Q&A

[Http://www.passcert.com](http://www.passcert.com)

We offer free update service for one year.

Exam : EX362

Title : Red Hat Certified Specialist
in Identity Management
exam

Version : DEMO

1.You must deploy a brand-new IdM realm using scripts on RHEL 9. Use integrated DNS and set Google Public DNS as a forwarder. Primary server: ipa1.example.com (10.10.10.11). Realm: EXAMPLE.COM, domain: example.com. Ensure services start at boot and verify the install.

A. See the Explanation.

Answer: A

Explanation:

1. Set hostname and basic resolution: `hostnamectl set-hostname ipa1.example.com`
`echo "10.10.10.11 ipa1.example.com ipa1" >> /etc/hosts`
2. Open firewall and install packages:
`dnf -y install ipa-server ipa-server-dns firewall-cmd --add-service={freeipa-ldap,freeipa-ldaps,dns} --permanent firewall-cmd --reload`
3. Run unattended install with integrated DNS: `ipa-server-install -U \`
`--realm EXAMPLE.COM --domain example.com \ --hostname ipa1.example.com \`
`--setup-dns --forwarder=8.8.8.8 \ --admin-password 'RedHat123!' \ --ds-password 'RedHat123!'`
4. Enable KRA (optional but commonly expected): `ipa-kra-install -p 'RedHat123!'`
5. Enable/verify services:
`systemctl enable --now ipa`
`kinit admin`
`ipa ping`
6. Validate DNS SRV and A records resolve: `dig +short _ldap._tcp.example.com SRV` `dig +short ipa1.example.com A`

2.Install the same IdM primary using Ansible Automation Platform (AAP) and the freeipa.ansible_freeipa collection, with integrated DNS and a forwarder.

A. See the Explanation.

Answer: A

Explanation:

1. On the control node, install the collection:
`ansible-galaxy collection install freeipa.ansible_freeipa`
2. Create inventory inventory.ini: `[ipaservers] ipa1.example.com`
`[all:vars]`
`ansible_user=root`
3. Create install-ipa.yml:

`- hosts: ipaservers`
`become: true collections:`
`- freeipa.ansible_freeipa roles:`
`- role: ipaserver`
`state: present`
`ipaserver_domain: example.com`
`ipaserver_realm: EXAMPLE.COM`
`ipaserver_setup_dns: true ipaserver_forwarders:`
`- 8.8.8.8`
`ipaserver_admin_password: "RedHat123!"`

ipaserver_dirman_password: "RedHat123!"

ipaserver_setup_kra: true

4. Run:

ansible-playbook -i inventory.ini install-ipa.yml

5. Post-check: kinit admin ipa config-show

ipa dnsconfig-show

3. Install an IdM server with external DNS (no integrated DNS). Configure global DNS forwarders afterwards from IdM.

A. See the Explanation.

Answer: A

Explanation:

1. Install IdM server without DNS: dnf -y install ipa-server ipa-server-install -U \

--realm EXAMPLE.COM --domain example.com \ --hostname ipa1.example.com \

--no-dns --admin-password 'RedHat123!' --ds-password 'RedHat123!'

2. Ensure external DNS has A/PTR and SRV records for IdM. At minimum (add in your external DNS):
ipa1.example.com. A 10.10.10.11

_kerberos._udp.example.com. SRV 0 100 88 ipa1.example.com. _kerberos._tcp.example.com. SRV 0

100 88 ipa1.example.com. _kpasswd._udp.example.com. SRV 0 100 464 ipa1.example.com.

_ldap._tcp.example.com. SRV 0 100 389 ipa1.example.com.

3. From IdM, set resolvers and forwarders (affects client-side DNS info served by SSSD/DNS discovery only if DNS integrated; otherwise for Kerberos discovery rely on SRV you created):

ipa config-mod --dns-forwarders=1.1.1.1 --dns-forwarders=8.8.8.8

4. Validate realm and KDC discovery:

ipa ping

5. Confirm clients can discover via SRV (from a client host): dig +short _ldap._tcp.example.com SRV

4. Perform a CA-less IdM deployment using an external corporate CA. Complete the two-stage process.

A. See the Explanation.

Answer: A

Explanation:

1. Stage 1: generate CSR: dnf -y install ipa-server

ipa-server-install --realm EXAMPLE.COM --domain example.com \

--hostname ipa1.example.com \

--no-ntp --external-ca -U \

--admin-password 'RedHat123!' --ds-password 'RedHat123!'

2. Collect CSR files (commonly /root/ipa.csr); submit to your external CA to obtain the server cert and the CA chain (PEM).

3. Stage 2: complete the install by providing the certs:

ipa-server-install --external-cert-file=/root/ipa_server_cert.pem \ --external-cert-file=/root/ca_chain.pem -

U

4. Start/enable and verify: systemctl enable --now ipa kinit admin

ipa cert-show 1

5.Enroll a RHEL client app1.example.com into the IdM realm, configure SSSD, and verify identity and sudo data retrieval.

A. See the Explanation.

Answer: A

Explanation:

1. Client prep:

```
hostnamectl set-hostname app1.example.com
```

```
echo "10.10.10.11 ipa1.example.com ipa1" >> /etc/hosts dnf -y install ipa-client sssd oddjob-mkhomedir
```

2. Run client install (use your server FQDN):

```
ipa-client-install -U --domain example.com --server ipa1.example.com \
```

```
--realm EXAMPLE.COM --mkhomedir --principal admin --password 'RedHat123!'
```

3. Validate identity lookup: getent passwd admin

```
id admin
```

4. Validate Kerberos and sudo: kinit admin

```
sudo -l
```

5. Ensure SSSD enabled: systemctl enable --now sssd