Installation of LDAP , Integrated DNS Server and Kerberos Server with FREE IPA Server Solution

Steps to configure LDAP(S) Server ,Integrated DNS Server and Kerberos server with FREE IPA server solution.

Commands :

yum install -y ipa-server bind-dyndb-ldap ipa-server-dns -To install all required packages

ipa-server-install -To install FreeIPA Server

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

Server host name [ipaserver.example.com]:**ipaserver.example.com**

Please confirm the domain name [example.com]:**example.com**

Please provide a realm name [EXAMPLE.COM]:**EXAMPLE.COM**

Directory Manager password:*********

Password (confirm):*********

IPA admin password:********

Password (confirm):*********

Do you want to configure DNS forwarders? [yes]:**no**

Do you want to search for missing the reverse zone? [yes]: **no**

Continue to configure the system with these values? [no]: **yes** (approximate 15-20 minutes)

firewall-cmd --permanent --add-service={ntp,http,https,ldap,ldaps,kerberos,dns} --permanent -To allow inbound traffic

firewall-cmd --reload -To reload the firewall

Managing DNS zones and DNS Record Entries

kinit admin -To authenticate as IPA Admin

Adding Reverse Zone :

ipa dnszone-add 122.168.192.in-addr.arpa. -To add Reverse zone by name

Adding Forward Zone :

ipa dnszone-add rhce.com - To create Forward zone for domain rhce.com

Adding Reverse Zone Entries for Machine's Hostnames :

ipa dnsrecord-add 122.168.192.in-addr.arpa. 254 --ptr-rec ipaserver.example.com. - Adding PTR record for 192.168.122.254

ipa dnsrecord-add 122.168.192.in-addr.arpa. 10 --ptr-rec server.example.com. - Adding PTR record for 192.168.122.10

ipa dnsrecord-add 122.168.192.in-addr.arpa. 20 --ptr-rec client.example.com. - Adding PTR record for 192.168.122.20

ipa dnsrecord-add 122.168.192.in-addr.arpa. 40 --ptr-rec client2.example.com. - Adding PTR record for 192.168.122.40

(Dont forget . At the end of above four commands)

Adding Forward Zone Entries Machine's Hostnames:

ipa dnsrecord-add example.com server --a-rec 192.168.122.10 -Adding A record for server.example.com

ipa dnsrecord-add example.com client --a-rec 192.168.122.20 -Adding A record for client.example.com

ipa dnsrecord-add example.com client2 --a-rec 192.168.122.40 -Adding A record for client2.example.com

Adding Forward Zone Entries for Virtual Hostnames and Web Server Names for Apache Web Server Objectives:

ipa dnsrecord-add example.com rhce --a-rec 192.168.122.10

ipa dnsrecord-add example.com web --a-rec 192.168.122.10

ipa dnsrecord-add example.com vhost1 --a-rec 192.168.122.10

ipa dnsrecord-add example.com group --a-rec 192.168.122.10

ipa dnsrecord-add example.com client12 --a-rec 192.168.122.10

ipa dnsrecord-add rhce.com client1_web --a-rec 192.168.122.10

ipa dnsrecord-add example.com nodef_port --a-rec 192.168.122.10

ipa dnsrecord-add example.com dynamic --a-rec 192.168.122.10

ipa dnsrecord-add example.com dynamicwsgi --a-rec 192.168.122.10

ipa dnsrecord-add example.com ssl --a-rec 192.168.122.10

ipa dnszone-show example.com -To query the DNS zone
host server.example.com -To query DNS for hostname(forward DNS lookup)
host 192.168.122.10 -To query DNS for IP (Reverse DNS lookup)

You can also use dig or nslookup utility for querying DNS Server

Don’t configure Reverse DNS lookup for Virtual Host and Web server names because in this way same IP address (192.168.122.10) will be mapped to multiple host names and will be conflicting for host access configurations of different services like SAMBA, Apache Web Server !!!

Creating LDAP users

kinit admin -To authenticate as IPA Admin

ipa user-add --homedir=/nfs/nfs1 --password -Creating user with non-default home directory

mkdir -p /nfs/nfs1 -To create non-default home directory

chown nfs1:nfs1 /nfs/nfs1 -To set user and group ownership to nfs1

ipa user-add --homedir=/nfs/nfs2 --password -Creating user with non-default home directory

mkdir -p /nfs/nfs2 -To create non-default home directory

chown nfs2:nfs2 /nfs/nfs2 -To set user and group ownership to nfs2

In similar way, You can add different users used in this course.

After configuring server and client machines to join KERBEROS Domain on ipaserver.example.com (We will do later in this course) , You will be able to use LDAP users on server and client machines.

But it will not be possible for LDAP user to get his home directory because for that you need to configure automount for home directories with autofs service. I assume you are already RHCSA and you know how to do this.

Adding Kerberos NFS Service principal on IPA Server for NFS Client(server.example.com)

kinit admin - To Authenticate as IPA Admin

ipa service-add nfs/server.example.com - To add NFS service principal