FreeIPA部署及基本使用

参考 https://www.cnblogs.com/sellsa/p/11087955.html

https://www.hadoop1024.com/2016/12/14/freeipa%E9%83%A8%E7%BD%B2%E6%AD%A5%E9%AA%A4/#FreeIPA-7

hostnamectl set-hostname freeipa.baofoo.cn

3、运行、停止、禁用firewalld

启动：# systemctl start firewalld

查看状态：# systemctl status firewalld 或者 firewall-cmd --state

停止：# systemctl disable firewalld

禁用：# systemctl stop firewalld

①安装ipa-server

```
yum install ipa-server bind bind-dyndb-ldap ipa-server-dns
```

②配置ipa-server

```
[root@freeipa ~]# ipa-server-install --setup-dns --allow-zone-overlap
```

```
Server host name [server.test.co]:     ---回车键（默认）

Please confirm the domain name [test.co]:    ---回车键（默认）

Please provide a realm name [TEST.CO]:  ---回车键（默认）

Directory Manager password:   ---设置目录管理的密码 最少是8位

IPA admin password:  ---设置ipa 管理员admin的密码 最少8位 一定要记住，后面要用到

Do you want to configure DNS forwarders? [yes]: no ---你想配置dns为转发器吗？ 选择no

Do you want to search for missing reverse zones? [yes]: yes --你想配置dns的反向域吗？选择yes

Continue to configure the system with these values? [no]: yes --继续配置系统其他的值？ 选择yes
```

部署客户端（client01.bigdata-hebona.com）

①修改客户端的DNS(网卡的配置)，然后重启网络

```
DNS1=192.168.48.128   #指向freeipa server
DNS2=114.114.114.114
```

②安装ipa-client

```
yum install -y ipa-client
```

②配置 client加入域

```
[root@client01 ~]# ipa-client-install
```

先在 vi /etc/hosts   增加freeipa server的主机名

```
[root@bigdata-5 ~]# ipa-client-install
DNS discovery failed to determine your DNS domain
Provide the domain name of your IPA server (ex: example.com): baofoo.cn
Provide your IPA server name (ex: ipa.example.com): freeipa.baofoo.cn
The failure to use DNS to find your IPA server indicates that your resolv.conf file is not
properly configured.
Autodiscovery of servers for failover cannot work with this configuration.
If you proceed with the installation, services will be configured to always access the
discovered server for all operations and will not fail over to other servers in case of
failure.
Proceed with fixed values and no DNS discovery? [no]: yes
Client hostname: bigdata-5.baofoo.cn
Realm: BAOFOO.CN
DNS Domain: baofoo.cn
IPA Server: freeipa.baofoo.cn
BaseDN: dc=baofoo,dc=cn

Continue to configure the system with these values? [no]: yes
Synchronizing time with KDC...
Attempting to sync time using ntpd.  Will timeout after 15 seconds
Unable to sync time with NTP server, assuming the time is in sync. Please check that 123
UDP port is opened.
User authorized to enroll computers: admin
Password for admin@BAOFOO.CN:
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=BAOFOO.CN
    Issuer:      CN=Certificate Authority,O=BAOFOO.CN
    Valid From:  2019-08-30 07:42:08
    Valid Until: 2039-08-30 07:42:08

Enrolled in IPA realm BAOFOO.CN
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm BAOFOO.CN
trying https://freeipa.baofoo.cn/ipa/json
[try 1]: Forwarding 'schema’ to json server 'https://freeipa.baofoo.cn/ipa/json’
trying https://freeipa.baofoo.cn/ipa/session/json
[try 1]: Forwarding 'ping’ to json server 'https://freeipa.baofoo.cn/ipa/session/json’
[try 1]: Forwarding 'ca_is_enabled’ to json server
'https://freeipa.baofoo.cn/ipa/session/json’
Systemwide CA database updated.
Hostname (bigdata-5.baofoo.cn) does not have A/AAAA record.
Failed to update DNS records.
Missing A/AAAA record(s) for host bigdata-5.baofoo.cn: 10.6.123.63.
Missing reverse record(s) for address(es): 10.6.123.63.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod’ to json server 'https://freeipa.baofoo.cn/ipa/session/json’
Could not update DNS SSHFP records.
SSSD enabled
Configured /etc/openldap/ldap.conf
No SRV records of NTP servers found. IPA server address will be used
NTP enabled
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring baofoo.cn as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
[root@bigdata-5 ~]#
```

添加用户 和组 、修改 **默认10分钟生效**

在freeip服务器上

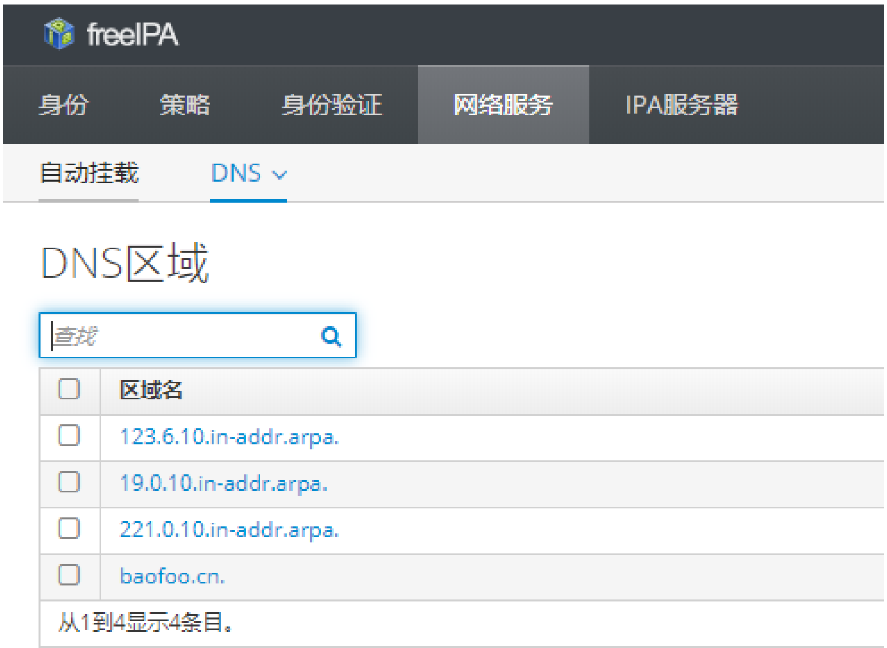
```
[root@freeipa ~]# vi /etc/sssd/sssd.conf

[nss]
memcache_timeout = 600
homedir_substring = /home
```

手动更新

```
  sss_cache  -u  yangze
```

添加客户端 和配置dns 没什么关系

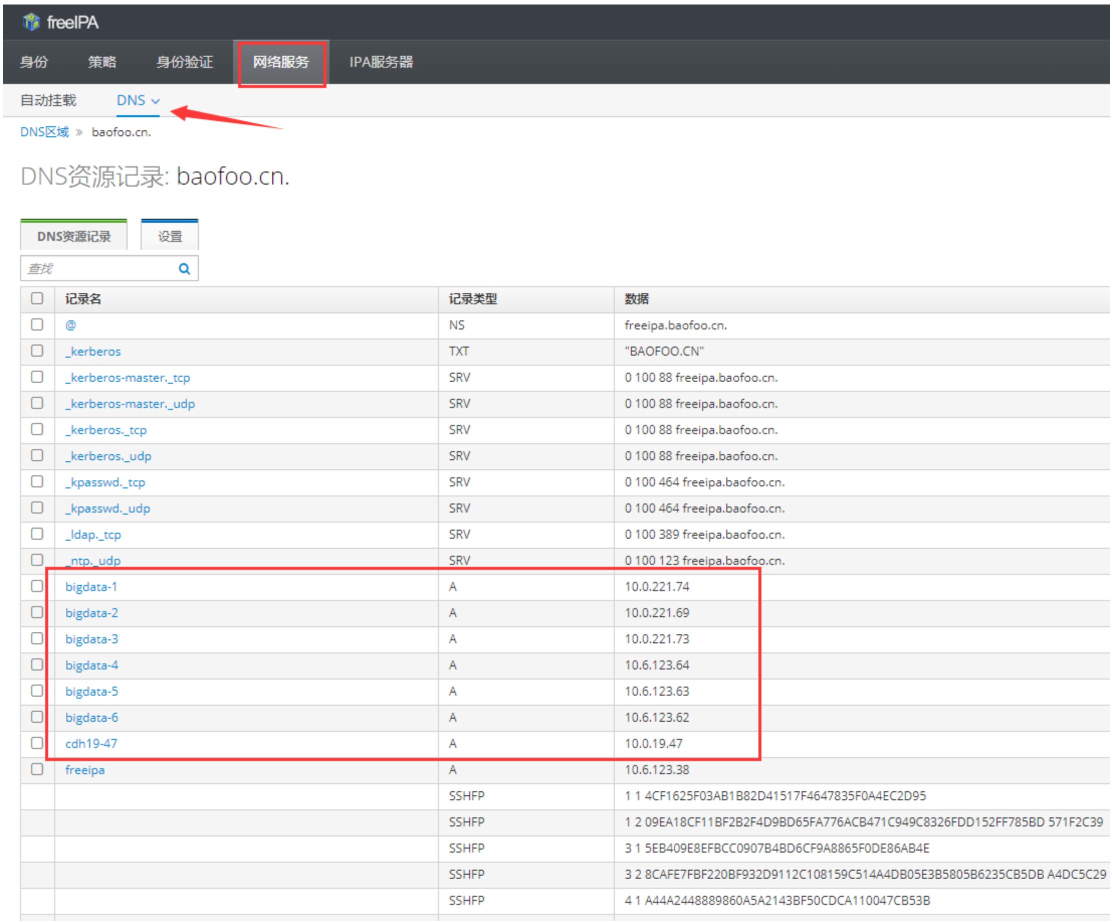
dns的使用



DNS区域

□	区域名
□	123.6.10.in-addr.arpa.
□	19.0.10.in-addr.arpa.
□	221.0.10.in-addr.arpa.
□	baofoo.cn.

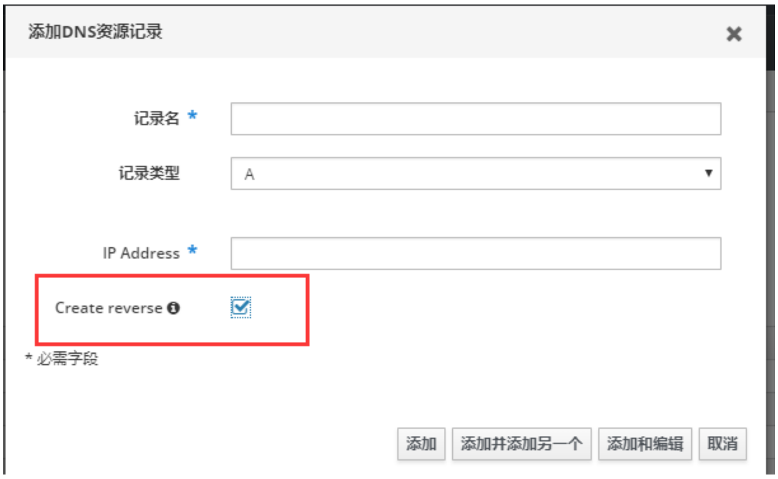
从1到4显示4条目。



DNS资源记录: baofoo.cn.

□	记录名	记录类型	数据
□	@	NS	freeipa.baofoo.cn.
□	_kerberos	TXT	"BAOFOO.CN"
□	_kerberos-master._tcp	SRV	0 100 88 freeipa.baofoo.cn.
□	_kerberos-master._udp	SRV	0 100 88 freeipa.baofoo.cn.
□	_kerberos._tcp	SRV	0 100 88 freeipa.baofoo.cn.
□	_kerberos._udp	SRV	0 100 88 freeipa.baofoo.cn.
□	_kpasswd._tcp	SRV	0 100 464 freeipa.baofoo.cn.
□	_kpasswd._udp	SRV	0 100 464 freeipa.baofoo.cn.
□	_ldap._tcp	SRV	0 100 389 freeipa.baofoo.cn.
□	_ntp._udp	SRV	0 100 123 freeipa.baofoo.cn.
□	bigdata-1	A	10.0.221.74
□	bigdata-2	A	10.0.221.69
□	bigdata-3	A	10.0.221.73
□	bigdata-4	A	10.6.123.64
□	bigdata-5	A	10.6.123.63
□	bigdata-6	A	10.6.123.62
□	cdh19-47	A	10.0.19.47
□	freeipa	A	10.6.123.38
		SSHFP	1 1 4CF1625F03AB1B82D41517F4647835F0A4EC2D95
		SSHFP	1 2 09EA18CF11BF2B2F4D9BD65FA776ACB471C949C8326FDD152FF785BD 571F2C39
		SSHFP	3 1 5EB409E8EFBCC0907B4BD6CF9A8865F0DE86AB4E
		SSHFP	3 2 8CAFE7FBF220BF932D9112C108159C514A4DB05E3B5805B6235CB5DB A4DC5C29
		SSHFP	4 1 A44A2448889860A5A2143BF50CDCA110047CB53B

记得添加反向记录（也就是ip能找到域名）



添加DNS资源记录

记录名 *

记录类型 A

IP Address *

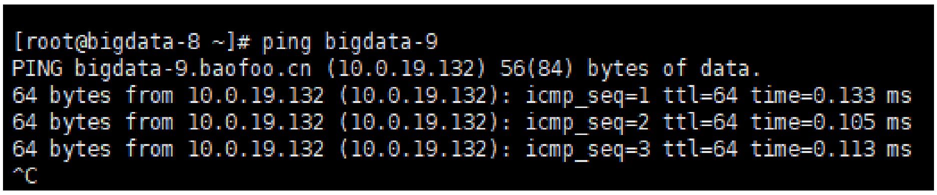
Create reverse ☑

* 必需字段

配好后 修改客户端的nameserver

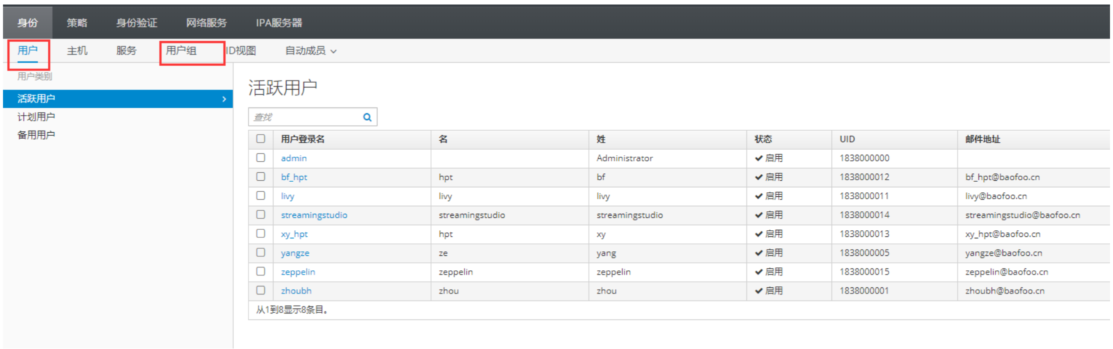
```
[root@bigdata-8 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
search baofoo.cn
#nameserver 202.96.209.5
#nameserver 202.96.209.133
nameserver 10.6.123.38
```

效果：



```
[root@bigdata-8 ~]# ping bigdata-9
PING bigdata-9.baofoo.cn (10.0.19.132) 56(84) bytes of data.
64 bytes from 10.0.19.132 (10.0.19.132): icmp_seq=1 ttl=64 time=0.133 ms
64 bytes from 10.0.19.132 (10.0.19.132): icmp_seq=2 ttl=64 time=0.105 ms
64 bytes from 10.0.19.132 (10.0.19.132): icmp_seq=3 ttl=64 time=0.113 ms
^C
```

ldap的使用

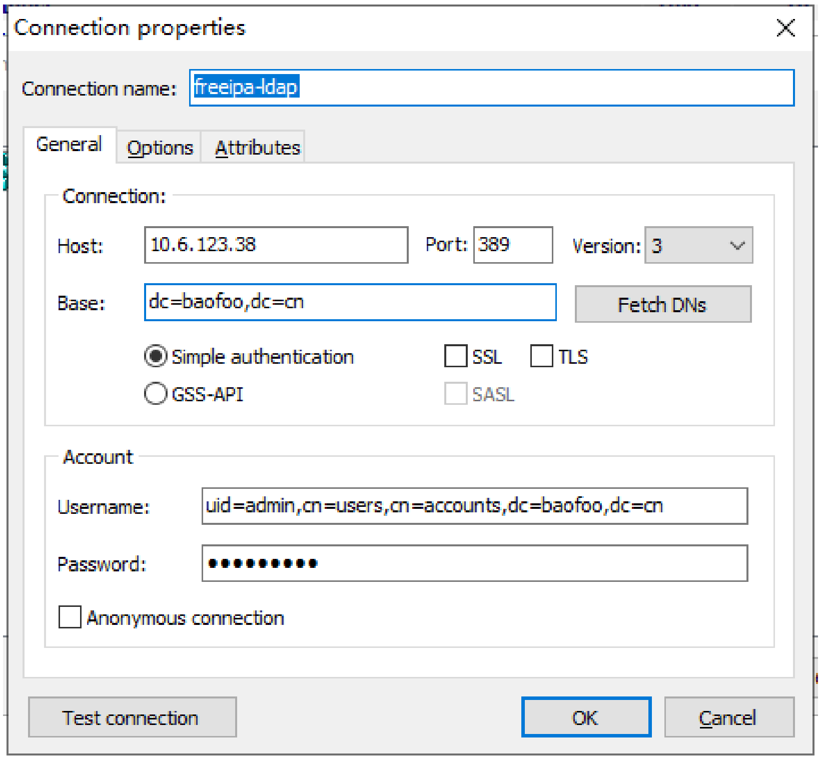


活跃用户

□	用户登录名	名	姓	状态	UID	邮件地址
□	admin		Administrator	✓ 启用	1838000000	
□	bf_hpt	hpt	bf	✓ 启用	1838000012	bf_hpt@baofoo.cn
□	livy	livy	livy	✓ 启用	1838000011	livy@baofoo.cn
□	streamingstudio	streamingstudio	streamingstudio	✓ 启用	1838000014	streamingstudio@baofoo.cn
□	xy_hpt	hpt	xy	✓ 启用	1838000013	xy_hpt@baofoo.cn
□	yangze	ze	yang	✓ 启用	1838000005	yangze@baofoo.cn
□	zeppelin	zeppelin	zeppelin	✓ 启用	1838000015	zeppelin@baofoo.cn
□	zhoubh	zhou	zhou	✓ 启用	1838000001	zhoubh@baofoo.cn

从1到8显示8条目。

uid=admin,cn=users,cn=accounts,dc=baofoo,dc=cn



Connection properties

Connection name: freeipa-ldap

Connection:

Host: 10.6.123.38 Port: 389 Version: 3

Base: dc=baofoo,dc=cn

● Simple authentication □ SSL □ TLS

○ GSS-API □ SASL

Account

Username: uid=admin,cn=users,cn=accounts,dc=baofoo,dc=cn

Password: •••••••••

□ Anonymous connection