Security: How do I install FreeIPA onto a Bright Cluster?

How do I install FreeIPA onto a Bright Cluster?

1. Install packages:

```
# yum -y install ipa-server
```

2. Stop LDAP server:

```
# cmsh -c "device services master; stop ldap"
```

3. change the default user portal port in the webserver SSL configuration file:

```
# vim /etc/httpd/conf.d/ssl.conf
```

Changing lines as indicated on a default installation will change the user portal port from 443 to 4443:

```
line 18: Listen 4443
line 74: <VirtualHost _default_:4443>
```

4. Set up FreeIPA:

```
# ipa-server-install --domain=cm.cluster --realm=CM.CLUSTER

The log file for this installation can be found in
/var/log/ipaserver-install.log
==============================================================================
========
This program will set up the IPA Server.

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)

To accept the default shown in brackets, press the Enter key.

Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com.


Server host name [adel70-c6.cm.cluster]:
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password:
```

```
Password (confirm):

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server
administration.

IPA admin password:
Password (confirm):


The IPA Master Server will be configured with:
Hostname:      adel70-c6.cm.cluster
IP address:    10.141.255.254
Domain name:   cm.cluster
Realm name:    CM.CLUSTER

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

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Configuring NTP daemon (ntpd)
  [1/4]: stopping ntpd
  [2/4]: writing configuration
  [3/4]: configuring ntpd to start on boot
  [4/4]: starting ntpd
Done configuring NTP daemon (ntpd).
Configuring directory server for the CA (pkids): Estimated time 30
seconds
  [1/3]: creating directory server user
  [2/3]: creating directory server instance
  [3/3]: restarting directory server
Done configuring directory server for the CA (pkids).
Configuring certificate server (pki-cad): Estimated time 3 minutes 30
seconds
  [1/21]: creating certificate server user
  [2/21]: creating pki-ca instance
  [3/21]: configuring certificate server instance
  [4/21]: disabling nonces
  [5/21]: creating CA agent PKCS#12 file in /root
  [6/21]: creating RA agent certificate database
  [7/21]: importing CA chain to RA certificate database
  [8/21]: fixing RA database permissions
  [9/21]: setting up signing cert profile
  [10/21]: set up CRL publishing
  [11/21]: set certificate subject base
  [12/21]: enabling Subject Key Identifier
  [13/21]: setting audit signing renewal to 2 years
  [14/21]: configuring certificate server to start on boot
```

```
  [15/21]: restarting certificate server
  [16/21]: requesting RA certificate from CA
  [17/21]: issuing RA agent certificate
  [18/21]: adding RA agent as a trusted user
  [19/21]: configure certificate renewals
  [20/21]: configure Server-Cert certificate renewal
  [21/21]: Configure HTTP to proxy connections
Done configuring certificate server (pki-cad).
Configuring directory server (dirsrv): Estimated time 1 minute
  [1/38]: creating directory server user
  [2/38]: creating directory server instance
  [3/38]: adding default schema
  [4/38]: enabling memberof plugin
  [5/38]: enabling winsync plugin
  [6/38]: configuring replication version plugin
  [7/38]: enabling IPA enrollment plugin
  [8/38]: enabling ldapi
  [9/38]: disabling betxn plugins
  [10/38]: configuring uniqueness plugin
  [11/38]: configuring uuid plugin
  [12/38]: configuring modrdn plugin
  [13/38]: enabling entryUSN plugin
  [14/38]: configuring lockout plugin
  [15/38]: creating indices
  [16/38]: enabling referential integrity plugin
  [17/38]: configuring ssl for ds instance
  [18/38]: configuring certmap.conf
  [19/38]: configure autobind for root
  [20/38]: configure new location for managed entries
  [21/38]: restarting directory server
  [22/38]: adding default layout
  [23/38]: adding delegation layout
  [24/38]: adding replication acis
  [25/38]: creating container for managed entries
  [26/38]: configuring user private groups
  [27/38]: configuring netgroups from hostgroups
  [28/38]: creating default Sudo bind user
  [29/38]: creating default Auto Member layout
  [30/38]: adding range check plugin
  [31/38]: creating default HBAC rule allow_all
  [32/38]: Upload CA cert to the directory
  [33/38]: initializing group membership
  [34/38]: adding master entry
  [35/38]: configuring Posix uid/gid generation
  [36/38]: enabling compatibility plugin
  [37/38]: tuning directory server
  [38/38]: configuring directory to start on boot
Done configuring directory server (dirsrv).
Configuring Kerberos KDC (krb5kdc): Estimated time 30 seconds
```

```
  [1/10]: adding sasl mappings to the directory
  [2/10]: adding kerberos container to the directory
  [3/10]: configuring KDC
  [4/10]: initialize kerberos container
  [5/10]: adding default ACIs
  [6/10]: creating a keytab for the directory
  [7/10]: creating a keytab for the machine
  [8/10]: adding the password extension to the directory
  [9/10]: starting the KDC
  [10/10]: configuring KDC to start on boot
Done configuring Kerberos KDC (krb5kdc).
Configuring kadmin
  [1/2]: starting kadmin
  [2/2]: configuring kadmin to start on boot
Done configuring kadmin.
Configuring ipa_memcached
  [1/2]: starting ipa_memcached
  [2/2]: configuring ipa_memcached to start on boot
Done configuring ipa_memcached.
Configuring the web interface (httpd): Estimated time 1 minute
  [1/13]: setting mod_nss port to 443
  [2/13]: setting mod_nss password file
  [3/13]: enabling mod_nss renegotiate
  [4/13]: adding URL rewriting rules
  [5/13]: configuring httpd
  [6/13]: setting up ssl
  [7/13]: setting up browser autoconfig
  [8/13]: publish CA cert
  [9/13]: creating a keytab for httpd
  [10/13]: clean up any existing httpd ccache
  [11/13]: configuring SELinux for httpd
  [12/13]: restarting httpd
  [13/13]: configuring httpd to start on boot
Done configuring the web interface (httpd).
Applying LDAP updates
```

6. Create a user:

```
[root@adel61-centos6 ~]# ipa user-add
First name: mohamed
Last name: adel
User login [madel]: adel
----------------
Added user "adel"
----------------
  User login: adel
  First name: mohamed
  Last name: adel
  Full name: mohamed adel
```

```
  Display name: mohamed adel
  Initials: ma
  Home directory: /home/adel
  GECOS field: mohamed adel
  Login shell: /bin/sh
  Kerberos principal: adel@CM.CLUSTER
  Email address: adel@cm.cluster
  UID: 401800001
  GID: 401800001
  Password: False
  Kerberos keys available: False
```

7. enable a user:

```
[root@adel61-centos6 ~]# ipa user-mod adel --password
Password:
Enter Password again to verify:
--------------------
Modified user "adel"
--------------------
  User login: adel
  First name: mohamed
  Last name: adel
  Home directory: /home/adel
  Login shell: /bin/sh
  Email address: adel@cm.cluster
  UID: 401800001
  GID: 401800001
  Account disabled: False
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
```

8. Configure the user portal to use the correct PAM module:

```
[root@adel61-centos6 ~]# cat /etc/pam.d/php
auth        sufficient    pam_sss.so
account        sufficient    pam_sss.so
```

Notes:

* The user portal will be accessible via port 4443:
https://hostname:4443

* The local LDAP service will no longer be functional, and so Bright cannot be used to manage users via `cmsh` or `cmgui` after deploying FreeIPA. Users should only be managed via FreeIPA after deploying FreeIPA.

* To configure the default shell for all users:

```
[root@adel61-centos6 ~]# ipa config-mod --defaultshell=/bin/bash
```

* To configure the shell for a particular user:

```
[root@adel61-centos6 ~]# ipa user-mod adel --shell=/bin/bash
```

Unique solution ID: #1215
Author: Frank Furter
Last update: 2014-08-12 12:54